Avaya Integrated Management 3.0

C360 Manager
User Guide

14-300164
Issue 2
June 2005

Copyright 2005, Avaya Inc.
All Rights Reserved

Notice

Every effort was made to ensure that the information in this document was complete and accurate at the time of printing. However, information is subject to change.

Warranty

Avaya Inc. provides a limited warranty on this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language as well as information regarding support for this product, while under warranty, is available through the following Web site: http://www.avaya.com/support.

Preventing Toll Fraud

"Toll fraud" is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there may be a risk of toll fraud associated with your system and that, if toll fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Fraud Intervention

If you suspect that you are being victimized by toll fraud and you need technical assistance or support, in the United States and Canada, call the Technical Service Center's Toll Fraud Intervention Hotline at 1-800-643-2353.

Disclaimer

Avaya is not responsible for any modifications, additions or deletions to the original published version of this documentation unless such modifications, additions or deletions were performed by Avaya. Customer and/or End User agree to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation to the extent made by the Customer or End User.

How to Get Help

For additional support telephone numbers, go to the Avaya support Web site: http://www.avaya.com/support. If you are:

- Within the United States, click the *Escalation Management* link. Then click the appropriate link for the type of support you need.
- Outside the United States, click the *Escalation Management* link. Then click the *International Services* link that includes telephone numbers for the international Centers of Excellence.

Providing Telecommunications Security

Telecommunications security (of voice, data, and/or video communications) is the prevention of any type of intrusion to (that is, either unauthorized or malicious access to or use of) your company's telecommunications equipment by some party.

Your company's "telecommunications equipment" includes both this Avaya product and any other voice/data/video equipment that could be accessed via this Avaya product (that is, "networked equipment").

An "outside party" is anyone who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf. Whereas, a "malicious party" is anyone (including someone who may be otherwise authorized) who accesses your telecommunications equipment with either malicious or mischievous intent.

Such intrusions may be either to/through synchronous (time-multiplexed and/or circuit-based), or asynchronous (character-, message-, or packet-based) equipment, or interfaces for reasons of:

- Utilization (of capabilities special to the accessed equipment)
- Theft (such as, of intellectual property, financial assets, or toll facility access)
- Eavesdropping (privacy invasions to humans)
- Mischief (troubling, but apparently innocuous, tampering)
- Harm (such as harmful tampering, data loss or alteration, regardless of motive or intent)

Be aware that there may be a risk of unauthorized intrusions associated with your system and/or its networked equipment. Also realize that, if such an intrusion should occur, it could result in a variety of losses to your company (including but not limited to, human/data privacy, intellectual property, material assets, financial resources, labor costs, and/or legal costs).

Responsibility for Your Company's Telecommunications Security

The final responsibility for securing both this system and its networked equipment rests with you - Avaya's customer system administrator, your telecommunications peers, and your managers. Base the fulfillment of your responsibility on acquired knowledge and resources from a variety of sources including but not limited to:

- Installation documents
- System administration documents
- Security documents
- Hardware-/software-based security tools
- Shared information between you and your peers
- Telecommunications security experts

To prevent intrusions to your telecommunications equipment, you and your peers should carefully program and configure:

- Your Avaya-provided telecommunications systems and their interfaces
- Your Avaya-provided software applications, as well as their underlying hardware/software platforms and interfaces
- Any other equipment networked to your Avaya products

TCP/IP Facilities

Customers may experience differences in product performance, reliability and security depending upon network configurations/design and topologies, even when the product performs as warranted.

Standards Compliance

Avaya Inc. is not responsible for any radio or television interference caused by unauthorized modifications of this equipment or the substitution or attachment of connecting cables and equipment other than those specified by Avaya Inc. The correction of interference caused by such unauthorized modifications, substitution or attachment will be the responsibility of the user. Pursuant to Part 15 of the Federal Communications Commission (FCC) Rules, the user is cautioned that changes or modifications not expressly approved by Avaya Inc. could void the user's authority to operate this equipment.

Product Safety Standards

This product complies with and conforms to the following international Product Safety standards as applicable:

Safety of Information Technology Equipment, IEC 60950, 3rd Edition, or IEC 60950-1, 1st Edition, including all relevant national deviations as listed in Compliance with IEC for Electrical Equipment (IECEE) CB-96A.

Safety of Information Technology Equipment, CAN/CSA-C22.2 No. 60950-00 / UL 60950, 3rd Edition, or CAN/CSA-C22.2 No. 60950-1-03 / UL 60950-1.

Safety Requirements for Information Technology Equipment, AS/NZS 60950:2000.

One or more of the following Mexican national standards, as applicable: NOM 001 SCFI 1993, NOM SCFI 016 1993, NOM 019 SCFI 1998.

The equipment described in this document may contain Class 1 LASER Device(s). These devices comply with the following standards:

- EN 60825-1, Edition 1.1, 1998-01
- 21 CFR 1040.10 and CFR 1040.11.

The LASER devices used in Avaya equipment typically operate within the following parameters:

Typical Center Wavelength	Maximum Output Power
830 nm - 860 nm	-1.5 dBm
1270 nm - 1360 nm	-3.0 dBm
1540 nm - 1570 nm	5.0 dBm

Luokan 1 Laserlaite

Klass 1 Laser Apparat

Use of controls or adjustments or performance of procedures other than those specified herein may result in hazardous radiation exposures. Contact your Avaya representative for more laser product information.

Electromagnetic Compatibility (EMC) Standards

This product complies with and conforms to the following international EMC standards and all relevant national deviations:

Limits and Methods of Measurement of Radio Interference of Information Technology Equipment, CISPR 22:1997, EN55022:1998, and AS/NZS 3548.

Information Technology Equipment - Immunity Characteristics - Limits and Methods of Measurement, CISPR 24:1997 and EN55024:1998, including:

- Electrostatic Discharge (ESD) IEC 61000-4-2
- Radiated Immunity IEC 61000-4-3
- Electrical Fast Transient IEC 61000-4-4
- Lightning Effects IEC 61000-4-5
- Conducted Immunity IEC 61000-4-6
- Mains Frequency Magnetic Field IEC 61000-4-8
- Voltage Dips and Variations IEC 61000-4-11

Power Line Emissions, IEC 61000-3-2: Electromagnetic compatibility (EMC) - Part 3-2: Limits - Limits for harmonic current emissions.

Power Line Emissions, IEC 61000-3-3: Electromagnetic compatibility (EMC) - Part 3-3: Limits - Limitation of voltage changes, voltage fluctuations and flicker in public low-voltage supply systems.

Federal Communications Commission Statement

Part 15:

*** Note:** This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Part 68: Answer-Supervision Signaling

Allowing this equipment to be operated in a manner that does not provide proper answer-supervision signaling is in violation of Part 68 rules. This equipment returns answer-supervision signals to the public switched network when:

- answered by the called station,
- answered by the attendant, or
- routed to a recorded announcement that can be administered by the customer premises equipment (CPE) user.

This equipment returns answer-supervision signals on all direct inward dialed (DID) calls forwarded back to the public switched telephone network. Permissible exceptions are:

- A call is unanswered.
- A busy tone is received.
- A reorder tone is received.

Avaya attests that this registered equipment is capable of providing users access to interstate providers of operator services through the use of access codes. Modification of this equipment by call aggregators to block access dialing codes is a violation of the Telephone Operator Consumers Act of 1990.

REN Number

For MCC1, SCC1, CMC1, G600, and G650 Media Gateways:

This equipment complies with Part 68 of the FCC rules. On either the rear or inside the front cover of this equipment is a label that contains, among other information, the FCC registration number, and ringer equivalence number (REN) for this equipment. If requested, this information must be provided to the telephone company.

For G350 and G700 Media Gateways:

This equipment complies with Part 68 of the FCC rules and the requirements adopted by the ACTA. On the rear of this equipment is a label that contains, among other information, a product identifier in the format US:AAAEQ##TXXXX. The digits represented by ## are the ringer equivalence number (REN) without a decimal point (for example, 03 is a REN of 0.3). If requested, this number must be provided to the telephone company.

For all media gateways:

The REN is used to determine the quantity of devices that may be connected to the telephone line. Excessive RENs on the telephone line may result in devices not ringing in response to an incoming call. In most, but not all areas, the sum of RENs should not exceed 5.0. To be certain of the number of devices that may be connected to a line, as determined by the total RENs, contact the local telephone company. REN is not required for some types of analog or digital facilities. Means of Connection

Connection of this equipment to the telephone network is shown in the following tables.

For MCC1, SCC1, CMC1, G600, and G650 Media Gateways:

Manufacturer's Port Identifier	FIC Code	SOC/REN/ A.S. Code	Network Jacks
Off premises station	OL13C	9.0F	RJ2GX, RJ21X, RJ11C
DID trunk	02RV2-T	0.0B	RJ2GX, RJ21X
CO trunk	02GS2	0.3A	RJ21X
	02LS2	0.3A	RJ21X
Tie trunk	TL31M	9.0F	RJ2GX
Basic Rate Interface	02IS5	6.0F, 6.0Y	RJ49C
1.544 digital interface	04DU9-BN	6.0F	RJ48C, RJ48M
	04DU9-IKN	6.0F	RJ48C, RJ48M
	04DU9-ISN	6.0F	RJ48C, RJ48M
120A4 channel service unit	04DU9-DN	6.0Y	RJ48C

For G350 and G700 Media Gateways:

Manufacturer's Port Identifier	FIC Code	SOC/ REN/ A.S. Code	Network Jacks
Ground Start CO trunk	02GS2	1.0A	RJ11C
DID trunk	02RV2-T	AS.0	RJ11C
Loop Start CO trunk	02LS2	0.5A	RJ11C
1.544 digital interface	04DU9-BN	6.0Y	RJ48C
	04DU9-DN	6.0Y	RJ48C
	04DU9-IKN	6.0Y	RJ48C
	04DU9-ISN	6.0Y	RJ48C
Basic Rate Interface	02IS5	6.0F	RJ49C

For all media gateways:

If the terminal equipment (for example, the media server or media gateway) causes harm to the telephone network, the telephone company will notify you in advance that temporary discontinuance of service may be required. But if advance notice is not practical, the telephone company will notify the customer as soon as possible. Also, you will be advised of your right to file a complaint with the FCC if you believe it is necessary.

The telephone company may make changes in its facilities, equipment, operations or procedures that could affect the operation of the equipment. If this happens, the telephone company will provide advance notice in order for you to make necessary modifications to maintain uninterrupted service.

If trouble is experienced with this equipment, for repair or warranty information, please contact the Technical Service Center at 1-800-242- 2121 or contact your local Avaya representative. If the equipment is causing harm to the telephone network, the telephone company may request that you disconnect the equipment until the problem is resolved.

A plug and jack used to connect this equipment to the premises wiring and telephone network must comply with the applicable FCC Part 68 rules and requirements adopted by the ACTA. A compliant telephone cord and modular plug is provided with this product. It is designed to be connected to a compatible modular jack that is also compliant. It is recommended that repairs be performed by Avaya certified technicians.

The equipment cannot be used on public coin phone service provided by the telephone company. Connection to party line service is subject to state tariffs. Contact the state public utility commission, public service commission or corporation commission for information.

This equipment, if it uses a telephone receiver, is hearing aid compatible.

Canadian Department of Communications (DOC) Interference Information

This Class A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

This equipment meets the applicable Industry Canada Terminal Equipment Technical Specifications. This is confirmed by the registration number. The abbreviation, IC, before the registration number signifies that registration was performed based on a Declaration of Conformity indicating that Industry Canada technical specifications were met. It does not imply that Industry Canada approved the equipment.

Installation and Repairs

Before installing this equipment, users should ensure that it is permissible to be connected to the facilities of the local telecommunications company. The equipment must also be installed using an acceptable method of connection. The customer should be aware that compliance with the above conditions may not prevent degradation of service in some situations.

Repairs to certified equipment should be coordinated by a representative designated by the supplier. Any repairs or alterations made by the user to this equipment, or equipment malfunctions, may give the telecommunications company cause to request the user to disconnect the equipment.

Declarations of Conformity

United States FCC Part 68 Supplier's Declaration of Conformity (SDoC)

Avaya Inc. in the United States of America hereby certifies that the equipment described in this document and bearing a TIA TSB-168 label identification number complies with the FCC's Rules and Regulations 47 CFR Part 68, and the Administrative Council on Terminal Attachments (ACTA) adopted technical criteria.

Avaya further asserts that Avaya handset-equipped terminal equipment described in this document complies with Paragraph 68.316 of the FCC Rules and Regulations defining Hearing Aid Compatibility and is deemed compatible with hearing aids.

Copies of SDoCs signed by the Responsible Party in the U. S. can be obtained by contacting your local sales representative and are available on the following Web site: http://www.avaya.com/support.

All Avaya media servers and media gateways are compliant with FCC Part 68, but many have been registered with the FCC before the SDoC process was available. A list of all Avaya registered products may be found at: http://www.part68.org by conducting a search using "Avaya" as manufacturer.

European Union Declarations of Conformity

CE

Avaya Inc. declares that the equipment specified in this document bearing the "CE" (*Conformité Europeénne*) mark conforms to the European Union Radio and Telecommunications Terminal Equipment Directive (1999/5/EC), including the Electromagnetic Compatibility Directive (89/336/EEC) and Low Voltage Directive (73/23/EEC).

Copies of these Declarations of Conformity (DoCs) can be obtained by contacting your local sales representative and are available on the following Web site: http://www.avaya.com/support.

Japan

This is a Class A product based on the standard of the Voluntary Control Council for Interference by Information Technology Equipment (VCCI). If this equipment is used in a domestic environment, radio disturbance may occur, in which case, the user may be required to take corrective actions.

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

To order copies of this and other documents:

Call: Avaya Publications Center
Voice 1.800.457.1235 or 1.207.866.6701
FAX 1.800.457.1764 or 1.207.626.7269

Write: Globalware Solutions
200 Ward Hill Avenue
Haverhill, MA 01835 USA
Attention: Avaya Account Management

E-mail: totalware@gwsmail.com

For the most current versions of documentation, go to the Avaya support Web site: http://www.avaya.com/support.

Table of Contents

Preface xi

The Purpose of This Guide xi
Who Should Use This Guide xi
Organization of This Guide xi

Chapter 1 — Introduction 1

Avaya C360 Manager Overview 1
Starting the Avaya C360 Manager 2
Avaya C360 Manager as Part of Avaya Integrated Management 2
Avaya C360 Manager via Web Management 3
The User Interface 4
Application Tabs 4
Status Line 5
Managing Tables 5

Chapter 2 — Device Manager 7

The User Interface 7
Application Toolbar 8
Get/Set Toolbar 10
Tree View 11
Desktop 11
Chassis View 12
Dialog Area 15
Avaya C360 Device Manager Modes 15
Refreshing Device Information 16
Using Dialog Boxes and Tables 16
Using Avaya C360 Device Manager Help 17
Opening the Help to the Contents Page 17
Opening the Help to a Topic of Interest 17

Chapter 3 — Device Configuration 19

Viewing Device Information 20
Device Information - General Tab 20
Device Information - Advanced Tab 21
Viewing Module Configuration 24
Module Configuration - General Tab 25
Module Configuration - Advanced Tab 28

Viewing LAG Configuration 31
LAG Configuration - General Tab 32
LAG Configuration - Advanced Tab 35
Viewing Port Configuration 39
Port Configuration - General Tab 40
Port Configuration - Advanced Tab 44
Port Configuration - LLDP Tab 48
Resetting the Device 51

Chapter 4 — Power over Ethernet 53

PoE Overview 53
Viewing PoE Information 54
Viewing PoE Port Information 54
Viewing PoE Configuration 54

Chapter 5 — G700 Media Gateway 59

G700 Media Gateway Overview 59
G700 Configuration 60
Viewing Module Configuration 60
Viewing Media Module Configuration 67
Avaya Site Administration 68

Chapter 6 — VoIP Engine Configuration 71

VoIP Overview 71
Configuring the VoIP Engine 71
VoIP Resources 72
VoIP Config 76
VoIP Status 77

Chapter 7 — WAN Configuration 79

X330WAN Overview 79
Avaya X330WAN Expansion Module Configuration 80
E1/T1 Port Configuration 81
Viewing Channel Group Information 84
Channel Group - PPP Session Information 84
Channel Group - Frame Relay Information 90
Managing Channel Groups 99
Viewing the Channel Groups Table 99
Creating, Editing, and Deleting Channel Groups 101
The Channel Group Wizard 101
USP Configuration 105
USP - PPP Interface 106
USP - Frame Relay Interface 114
Backup Interface Configuration 122
Viewing the Backup Interfaces Table 122
The Backup Interface Wizard 124

Chapter 8 — Port RMON 131

Displaying the Port RMON Window 132
The Pie Chart 132
The Traffic Graph 132
Traffic Types 133

Chapter 9 — VLANs 135

VLAN Configuration Overview 135
VLANs Overview 136
Master VLAN List 136
VLAN Tags 136
Viewing the VLAN Configuration Dialog Box 137
VLAN Tree 138
Selection List 139
Port Configuration Area 140
Managing VLANs 142
Creating VLANs 142
Renaming VLANs 143
Synchronizing VLAN Names 144
Deleting VLANs 145
Managing Port VLAN Settings 145
Selecting Ports 145
Viewing Port VLAN Settings 146
Using the Port Configuration Area 146
Drag-and-Drop 147
Updating the Device 147

Chapter 10 — Link Aggregation Groups 149

LAGs Overview 149
Viewing the LAG Table 150
Creating LAGs 151
Editing LAGs 151
The LAG Wizard 151
Welcome Screen 152
Base Port Selection Screen 153
Member Port Selection Screen 154
LAG Name Screen 155
Confirmation Screen 156
Deleting LAGs 157

Chapter 11 — Port Redundancy 159

Overview of Port Redundancy 159
Viewing the Port Redundancy Dialog Box 160
Adding a Port Redundancy 162
Port Redundancy Wizard 163
Welcome Screen 164

Primary Port Selection Screen 165
Secondary Port Selection Screen 166
Name and Type Screen 167
Confirmation Screen 168
Deleting Port Redundancies 169
Updating the Device 169

Chapter 12 — Port Mirroring 171

Port Mirroring Overview 171
Configuring Port Mirroring 171
The Port Mirroring Wizard 172
Create Welcome Screen 173
Edit/Delete Welcome Screen 174
Source Port Selection Screen 175
Destination Port Selection Screen 176
Frames Direction Selection Screen 177
Confirmation Screen 178

Chapter 13 — IP Multicast Filtering 179

IP Multicast Filtering Overview 179
Configuring IP Multicast Filtering 180

Chapter 14 — Trap Managers Configuration 183

Trap Manager Overview 183
Viewing the Stack Trap Managers Table 184
Stack Trap Manager Table - SNMPv1 Legacy Tab 184
Stack Trap Managers Table - SNMPv3 Tab 186
Viewing the Media Gateway Trap Managers Table 189
Viewing the WAN Trap Managers Table 191
Editing the Trap Managers Table 193
Adding and Removing Managers 193
Editing Trap Reporting Statuses 193

Chapter 15 — Switch Connected Addresses 195

Switch Connected Addresses Overview 195
Viewing the Switch Connected Addresses Window 196
Sorting the List of Stations 197

Chapter 16 — Port Security. 199

802.1x Port Security 199
802.1x Port Security Overview 199
Configuring 802.1x Port Security 200
MAC Port Security 203
MAC Port Security Overview 203
Configuring MAC Port Security 203

Chapter 17 — Routing Manager 207

Router Modes 208
Router 208
Layer 2 Switch 208
The User Interface 209
Toolbar 210
Tree View 211
Table Area 212
Form Area 212
Editing Tables 213
Saving Table Information as Text 214
Saving Configuration Changes 214
Running Changes 214
Committed Changes 214
Resetting a Router 215
Using Avaya C360 Routing Manager Help 215
Opening the Help to the Contents Page 215
Opening the Help to a Topic of Interest 215

Chapter 18 — Device 217

Device Global Parameters 217

Chapter 19 — Layer 2 219

VLANs 219

Chapter 20 — IP Route 221

IP Global Parameters 222
IP Interfaces 223
Routing Table 225
ARP Table 229
DHCP 231
DHCP/BOOTP Global Parameter 231
DHCP/BOOTP Parameters 232
RIP 234
RIP Global Parameters 234
RIP Interfaces 236
OSPF 239
OSPF Global Parameters 239
OSPF Interfaces 241
OSPF Area Parameters 243
OSPF Link State Database 244
OSPF External Database 246
OSPF Neighbors 247
VRRP 248
VRRP Global Parameters 249
VRRP Table 250

CRTP 253
CRTP Interfaces 253

Appendix A — Menus 255

Device Manager Menus 255
File Menu 255
View Menu 255
Configure Menu 256
Actions Menu 256
Tools Menu 257
Help Menu 257
Routing Manager Menus 258
File Menu 258
Edit Menu 258
View Menu 258
Action Menu 259
Help Menu 259

Appendix B — Web Management 261

Web Management Overview 261
Configuring the Avaya C360 Device 261

Index 263

Preface

Welcome to Avaya C360 Manager. This chapter provides an introduction to the structure and assumptions of this guide. It includes the following sections:

- **The Purpose of This Guide** - A description of the goals of this guide.
- **Who Should Use This Guide** - The intended audience of this guide.
- **Organization of This Guide** - A brief description of the subjects contained in the various sections of this guide.

The Purpose of This Guide

The Avaya C360 Manager guide contains information needed to use the management system efficiently and effectively.

Who Should Use This Guide

This guide is intended for network managers familiar with network management and its fundamental concepts.

Organization of This Guide

This guide is structured to reflect the following conceptual divisions:

- **Avaya C360 Manager** - Information pertaining to the entire Avaya C360 Manager application and all of its aspects.
  - **Preface** - This section describes the guide's purpose, intended audience and organization.
  - **Introduction** - An introduction to the Avaya C360 Manager including instructions on starting the Avaya C360 Manager.

- **Avaya C360 Device Manager** - Information pertaining to Avaya C360 Device management.
  - **Device Manager** - An introduction to the Avaya C360 Device Manager including a description of the user interface.
  - **Device Configuration** - Viewing and modifying the different device configurations.
  - **Power Over Ethernet** - An overview of Power over Ethernet (PoE) and instructions on viewing and configuring PoE parameters.
  - **G700 Media Gateway** - An overview of the G700 Media Gateway and information on viewing and configuring G700 components.
  - **VoIP Engine Configuration** - An overview of VoIP Engine functionality and information on viewing and configuring VoIP Engine parameters.
  - **WAN Configuration** - An overview of the Avaya X330WAN expansion module functionality and information on viewing and configuring WAN parameters.
  - **Port RMON** - Viewing graphical representations of the traffic on the ports of the Avaya C360 Device.
  - **VLANs** - Viewing and editing VLAN information.
  - **Link Aggregation Groups (LAGs)** - Viewing and editing LAG information.
  - **Port Redundancy** - Configuring port redundancy for ports and LAGs in an Avaya C360 Device.
  - **Port Mirroring** - Setting up port mirroring for ports and LAGs in an Avaya C360 Device.
  - **IP Multicast Filtering** - Viewing and modifying IP Multicast filtering in an Avaya C360 Device.
  - **Trap Managers Configuration** - Viewing and modifying the Trap Managers table.
  - **Switch Connected Addresses** - Viewing devices connected to selected ports.
  - **Port Security** - Viewing and modifying port security settings.

- **Avaya C360 Routing Manager** - Information pertaining to Avaya C360 routing management.
  - **Routing Manager** - An introduction to configuring routing with Avaya P330ML and Avaya C360 modules, and a description of the Avaya C360 Routing Manager user interface.
  - **Device** - Detailed descriptions of routing device configuration that enable you to display and modify global parameters, reset the module, and upload or download configuration parameters.
  - **Layer 2** - Detailed descriptions of layer 2 configuration that enable you to view layer 2 interfaces at the management station.
  - **IP Route** - Detailed descriptions of IP route configuration that enable you to display and update IP interfaces, the IP routing table, the ARP table, DHCP/BOOTP parameters, RIP interfaces, OSPF interfaces, area parameters, link-state database and neighbors, the IP access control table, and redundancy parameters.
- **Appendices** - Additional information about the Avaya C360 Manager.
  - **Menus** - The full structure of the menus in the Avaya C360 Manager.
  - **Web Management** - Instructions on how to manage Avaya C360 Devices via the Internet.

1 Introduction

This chapter provides an introduction to the Avaya C360 Manager. It includes the following sections:

- **Avaya C360 Manager Overview** - An overview explaining the different aspects of Avaya C360 Device management.
- **Starting the Avaya C360 Manager** - Instructions on how to access Avaya C360 Manager from your management platform.
- **The User Interface** - Detailed descriptions of the user interface common to all applications in the Avaya C360 Manager.
- **Managing Tables** - An explanation of the symbols used to label table rows.

Avaya C360 Manager Overview

The Avaya C360 Manager provides full management capabilities for Avaya C360 Devices. This includes the ability to view three aspects of device management:

- **Device Manager** - Provides a view of the configuration of the device including VLAN configuration, configured LAGs, port mirroring, and traps. For information specific to the Avaya C360 Device Manager, refer to chapters 2-17.
- **Routing Manager** - Provides a view of the third layer routing and forwarding functions of the device. For information specific to the Avaya C360 Routing Manager, refer to chapters 18-22.
- **Device SMON** - Provides advanced monitoring capabilities for the device. For information specific to Avaya C360 SMON, refer to *Avaya C360 SMON User Guide*.

For information on switching between the different views, refer to "Application Tabs" on page 4.

Starting the Avaya C360 Manager

This section provides instructions for starting Avaya C360 Manager.

Avaya C360 Manager as Part of Avaya Integrated Management

If you installed the Avaya C360 Manager as part of Avaya Integrated Management, the following sections provide instructions for starting Avaya C360 Manager.

Running Avaya C360 Manager from Avaya Network Management Console

From the management platform map:

1. Select the label representing the Avaya C360 Device you want to manage.
2. Click .

   Or

   Double-click the Avaya C360 Device.

   Or

   Select **Tools > Avaya Device Manager**.

Running Avaya C360 Manager from HP NNM

From the management platform map:

1. Select the Avaya C360 Device you want to manage.
2. Click in the OpenView toolbar.

   Or

   Select **Tools > Avaya > Avaya Device Manager.**

Or

1. Right-click the Avaya C360 Device you want to manage.
2. Select **Avaya > Device Manager**.

Avaya C360 Manager via Web Management

To start Avaya C360 Web Management:

1. Point your web browser to **http://**xxx.xxx.xxx.xxx, where xxx.xxx.xxx.xxx is the IP address of the Avaya C360 Device you want to manage. The Network Password dialog box opens.

Figure 1-1. Network Password Dialog Box

2. For SNMPv1 login, enter the SNMP community string.

   Or

   For SNMP v3 login:

   Enter the User Name.

   Enter the Authentication password.

   Enter the Privacy password.

3. Click **OK**. The Avaya C360 Welcome page opens.

   — If the required Java plug-in is installed on your computer, the Java Plug-in Security Warning dialog box opens after a few seconds.

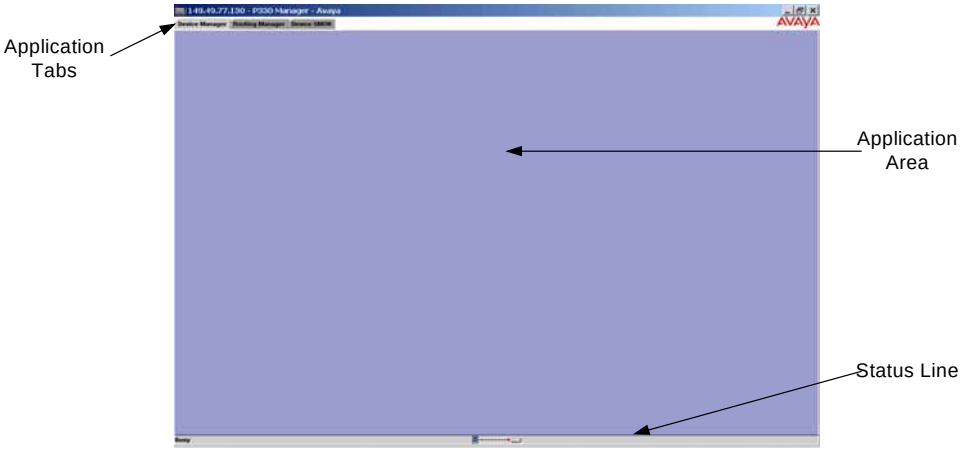
   — If the required Java plug-in is not installed, the plug-in is automatically downloaded to your computer. Follow the instructions on the Avaya C360 Welcome page to install the plug-in.

The User Interface

The Avaya C360 Manager user interface is different for each of its management applications. However, the following elements of the user interface are common to all views:

- **Application Tabs** - Tabs for accessing the Device Manager, Routing Manager, and SMON applications for the Avaya C360 Device.
- **Application Area** - An area where the selected application opens.
- **Status Line** - Displays the communication status between the Avaya C360 Manager and the Avaya C360 Device.

Figure 1-2. Avaya C360 Manager User Interface



Application Tabs

You can access the three main components of device management using the following Application Tabs in the Avaya C360 Manager:

- **Device Manager** - View the Avaya C360 Device Manager for device configuration and Port RMON.
- **Device SMON** - View SMON (Switch Monitoring) information for the Avaya C360 Device.
- **Routing Manager** - View the Avaya C360 Routing configuration.

To switch to a different view, click the appropriate Application Tab. The selected application opens.

*** Note:** When the Avaya C360 Manager is installed as a standalone manager and when running the Avaya C360 Manager via Web Management, the Device SMON and AnyLayer SMON tabs do not appear.

Status Line

The Status Line shows the communication status between the application and the Avaya C360 Device. The Status Line displays a status message and an appropriate graphic. The table below shows the possible statuses with their corresponding graphics, and provides an explanation for each status.

Table 1-1. Communication Statuses

Status	Graphic	Description
Ready		The application is ready to communicate with the Avaya C360 Device.
Communicating		The application is currently communicating with the Avaya C360 Device.
Communication Error		The last attempted communication with the Avaya C360 Device was not successful.

Managing Tables

The Avaya C360 Manager interface displays the status of each row in a table. The following table shows a list of symbols that can appear at the start of a table row, with their corresponding explanations.

Table 1-2. Table Symbols

Symbol	Explanation
	The row is a new entry.
	The row is to be deleted.
	The information in the row has been changed by the user.

To undo all the changes made to a table, click **Refresh**. To undo changes made to a selected row, click **Undo**. When all changes are finalized, click **Apply** to update the device.

2 Device Manager

This chapter provides an introduction to the Avaya C360 Device Manager. It includes the following sections:

- **The User Interface** - An introduction to the Avaya C360 Device Manager user interface, including instructions for selecting elements and using the toolbar buttons.
- **Avaya C360 Device Manager Modes** - Instructions on switching between the configuration and Port RMON modes in the Avaya C360 Device Manager.
- **Refreshing Device Information** - Instructions on how to refresh the information in the Avaya C360 Manager.
- **Using Dialog Boxes and Tables** - An explanation of the icons found in the dialog boxes and tables in the Avaya C360 Device Manager.
- **Using Avaya C360 Device Manager Help** - An explanation of the options for accessing on-line help in the Avaya C360 Device Manager.

The User Interface

The Avaya C360 Device Manager user interface consists of the following elements:

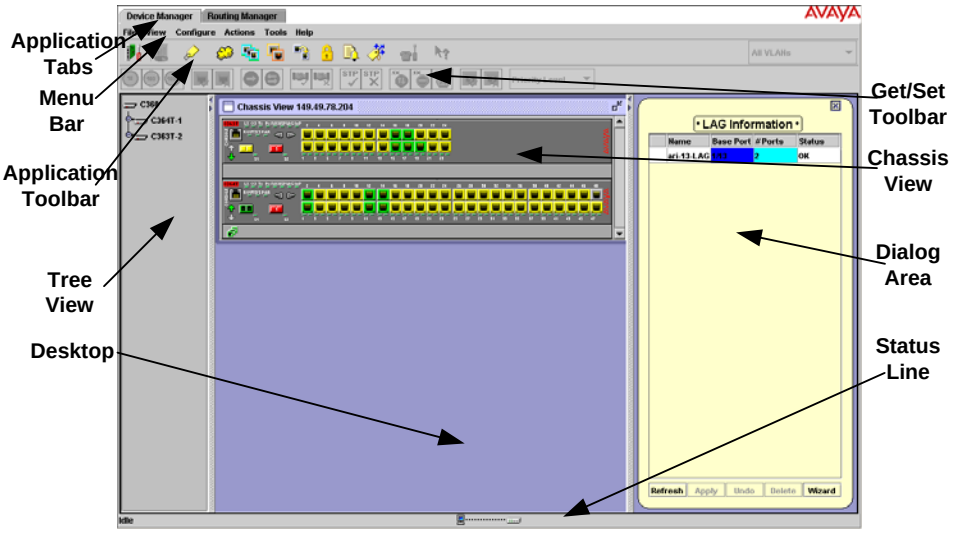
- **Menu Bar** - Menus for accessing Avaya C360 Device management functions.
- **Application Toolbar** - Toolbar buttons for accessing Avaya C360 Device management functions.
- **Get/Set Toolbar** - Toolbar buttons for viewing and changing the configuration of ports and LAGs.
- **Tree View** - A resizeable window containing a hierarchical representation of the modules and ports of the Avaya C360 Device.
- **Desktop** - A resizeable window where the Chassis View and all floating and minimized dialog boxes and tables are displayed.

- **Chassis View** - A graphical representation of the Avaya C360 Device.
- **Dialog Area** - A resizeable window where all dialog boxes and tables first open.

For information on other parts of the user interface, refer to "The User Interface" on page 4.

The figure below shows the user interface, with its various parts labeled.

Figure 2-1. The Avaya C360 Device Manager User Interface



To resize the three main areas of the user interface, the Tree View, the Chassis View, and the Dialog Area, use the splitter bars and their arrows.

Application Toolbar

The Application Toolbar provides shortcuts to the main Device Manager functions.

The table below describes the buttons on the Application Toolbar and gives the equivalent menu options.

Table 2-1. Application Toolbar

Button	Description	Menu Item
	Sets the device manager to Configuration Mode.	**View > Configuration**
	Sets the device manager to Port RMON mode.	**View > Port RMON**

Table 2-1. Application Toolbar (Continued)

Button	Description	Menu Item
	Displays addresses of devices connected to the switch.	**View > Switch Connected Addresses**
	Displays the VLAN window.	**Configure > VLAN**
	Displays the LAG table.	**Configure > LAG**
	Displays the Port Redundancy table.	**Configure > Port Redundancy**
	Starts the Port Mirroring wizard.	**Configure > Port Mirroring**
	Displays the MAC Port Security configuration.	**Configure > MAC Port Security**
	Displays the Trap Manager Table.	**Configure > Trap Managers**
	Displays the IP Multicast Filtering dialog box.	**Configure > IP Multicast Filtering**
	Launches Avaya Call Processing on the selected G700 Media Gateway or Voice port.	**Tools > Administer Station/Gateway**
	Opens the on-line help.	**Help > Help On**
	Selects a VLAN. Ports that are not on the selected VLAN appear dark gray in the Chassis View.	

When you place the cursor on a toolbar icon for one second, a label appears with the name of the button.

You can toggle the display of the application toolbar. To toggle the display of the application toolbar, select **View > Toolbars > Show Application Toolbar**.

Get/Set Toolbar

The Get/Set Toolbar provides buttons for getting and setting configuration parameters for selected ports and LAGs. When a port or LAG is selected, its configuration is reflected on the Get/Set Toolbar. Each group of buttons represents the various possible states of a configuration parameter. For example, the first group of buttons represents the possible speed of a port - 10 Mbps, 100 Mbps, or 1000 Mbps. If the center button is depressed, the port is currently configured to operate at 100 Mbps.

Selected ports and LAGs can be configured using the Get/Set Toolbar. To change the configuration of a port or LAG, click the button which represents the value of the parameter you want to apply to the port or LAG. Click **apply** to update the device with the changes. Click **cancel** to discard the changes. Options not applicable to the selected port or LAG are dimmed.

To configure the ports of a LAG, select the LAG icon in the Tree View or the Chassis View. Ports belonging to a LAG may not be configured by selecting the port.

Multiple ports and LAGs can be simultaneously configured using the Get/Set Toolbar. When multiple ports or LAGs with non-identical configurations are selected, only the parameters whose settings are identical on the selected ports or LAGs are reflected in the Get/Set Toolbar. For example, if a port operating at full duplex and a port operating at half duplex are selected, neither of the duplex mode buttons on the Get/Set Toolbar are depressed.

The table below displays the buttons on the Get/Set Toolbar and explains their functions and settings.

Table 2-2. Get/Set Toolbar

Button	Description
	Get and set the port/LAG's speed: 10 Mbps, 100 Mbps, 1000 Mbps.
	Get and set the port/LAG's status: Enabled, Disabled.
	Get and set the port/LAG's mode: Half duplex, Full duplex.
	Get and set the port/LAG's auto-negotiation status: Auto-negotiation Enabled, Auto-negotiation Disabled.
	Get and set the port/LAG's STP mode: Enabled, Disabled.

Table 2-2. Get/Set Toolbar (Continued)

Button	Description
	Get and set the port's 802.1x mode: 802.1x Force Authorized, 802.1x Force Unauthorized, 802.1x Auto.
	Get and set the port's Power over Ethernet
	Get and set the port/LAG's priority. Select a priority level between 1 and 8 using the pull-down listbox.
	Apply or cancel the configuration changes made with the Get/Set Toolbar.

You can toggle the display of the Get/Set toolbar. To toggle the display of the Get/Set toolbar, select **View > Toolbars > Show Get/Set Toolbar**.

Tree View

The Tree View shows a hierarchical representation of the structure of the Avaya C360 Device. To select ports, LAGS, modules or media modules, click their icons in the Tree View. When an element is selected in the Tree View, the corresponding element is selected in the Chassis View.

The highest level of the Tree View represents the device. The second level shows modules. The third level shows ports and LAGs. This includes ports on expansion modules.

To expand the view of a contracted element in the tree or to contract the view of an expanded element in the tree:

Double-click the element.

Or

Click the handle next to the element you want to expand or contract.

Desktop

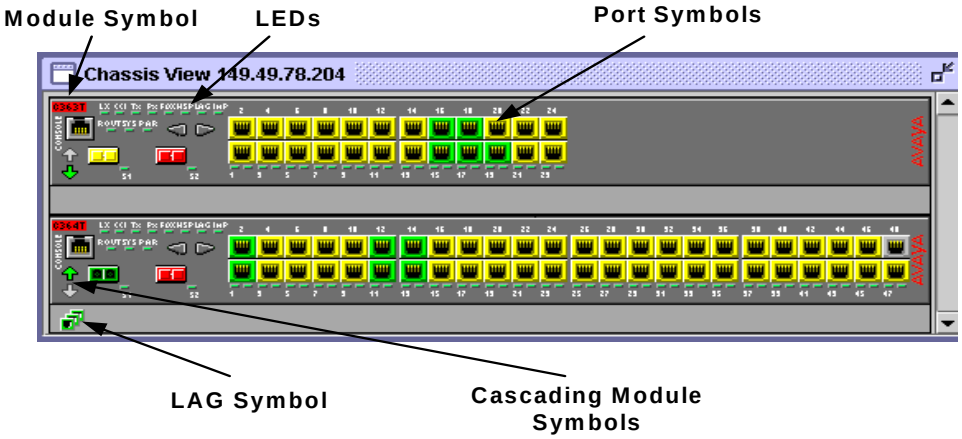
The central section of the application window is the Desktop. This area can be resized by dragging the vertical splitter bars with the mouse. Floating dialog boxes and tables can be resized. The Chassis View and floating dialog boxes and tables can also be minimized. Minimized windows appear at the bottom of the Desktop.

Chassis View

The Chassis View is a graphical representation of the Avaya C360 Device. The Avaya C360 Device can contain several Avaya C360 modules. The Chassis View shows all of the device's modules, LAGs, and ports, including ports on expansion modules and cascading modules (when present). The colors of the modules, LAGs, and ports in the Chassis View reflect their status.

When you hold the cursor over a port's icon in the Chassis View, a label appears with the port number, its VLAN ID, and the last fault that occurred on the port. When you hold the cursor over a LAG's icon in the Chassis View, a label appears with the name and VLAN number of the LAG, and the last fault that occurred on the LAG.

Figure 2-2. Avaya C360 Chassis View



When viewing selected dialog boxes, the color of the port or LAG indicates the status of the port or LAG with regard to the application. For example: When creating a Link Aggregation Group (LAG), ports that can be selected appear white in the Chassis View. The port selected to be the base port appears dark blue. The ports selected to be additional ports appear cyan.

The Cascading Module symbols show the status of the links between adjacent modules in the device. The Cascading Module symbols at the top and bottom of the device show the status of the long cable link between the top and bottom modules in the device. If there is no Cascading Module in the device, the Cascading Module symbols do not appear.

The following table provides a list of the possible port and LAG colors in the Chassis View and their meaning.

Table 2-3. Chassis View Port/LAG Colors

Color	Meaning
Green	The port/LAG is enabled, and its status is Okay.
Yellow	The port/LAG is enabled, and its status is Warning.
Red	The port/LAG is enabled, and its status is Fatal.
Light Gray	The port/LAG is disabled.
Dark Gray	The port/LAG is not associated with the assignment.
White	The port/LAG is logically available for assignment.
Dark Blue	The port/LAG has been assigned the primary position in an application.
Cyan	The port/LAG has been assigned a secondary position in an application.

GBIC Ports

Some Avaya C360 expansion modules contain GBIC (GigaBit Interface Converter) ports that house removable transceiver modules. The Chassis View reflects the management status of the ports. The following table shows the possible appearances of these ports in the Chassis View and provides the corresponding management status of the port.

Table 2-4. GBIC Port Status

GBIC Port	Status
	The GBIC port contains a supported transceiver module.
	There is no transceiver module present in the GBIC port.
	The transceiver module in the GBIC port is not supported.
	The transceiver module in the GBIC port is of an unknown type.

GBIC ports that contain the following types of transceiver modules can be configured:

- Supported transceiver modules
- No transceiver modules
- Unknown transceiver modules

GBIC ports that contain unsupported transceiver modules cannot be configured.

Selecting Elements

You can select modules, LAGs, and ports.

To select a module:

In the Chassis View, click the module's label.

Or

In the Tree View, click the module's icon. The module's label is highlighted in the Chassis View and the Tree View.

To select a LAG:

In the Chassis View, click the LAG's icon.

Or

In the Tree View, click the LAG's icon. The LAG is highlighted in the Chassis View and the Tree View.

To select a port:

In the Chassis View, click the port.

Or

In the Tree View, click the port's icon. The port is highlighted in the Chassis View and the Tree View.

— To select multiple elements, press **CTRL** while clicking on each element to be selected.

Dialog Area

The area to the right of the Chassis View is where all dialog boxes, tables, and wizards first appear. This area can be resized by dragging the vertical splitter bar with the mouse. When a dialog box, table, or wizard opens, it replaces the current dialog box open in the Dialog Area. To view more than one dialog box or table simultaneously, click the pushpin in the upper right-hand corner of the dialog box. The dialog box becomes a floating dialog box and moves to the Desktop.

To restore a dialog box to the Dialog Area, click the toolbar button or icon that opened the dialog box. The dialog box returns to the Dialog Area.

Avaya C360 Device Manager Modes

The Avaya C360 Device Manager has two modes:

- Configuration mode
- Port RMON mode

When in configuration mode, you can view and change the configuration of the Avaya C360 Device and individual ports. When in Port RMON mode, you can view graphical representations of the traffic on individual ports.

To switch to configuration mode:

Click .

Or

Select **View > Configuration**.

To switch to Port RMON mode:

Click .

Or

Select **View > Port RMON**.

Refreshing Device Information

You can refresh the information in the Avaya C360 Device Manager. To refresh Avaya C360 device information, select **View > Refresh**. The Avaya C360 Device Manager refreshes its device information and updates the display.

Using Dialog Boxes and Tables

Dialog boxes and tables in the Avaya C360 Manager application have a common set of buttons. The following table displays the buttons and explains their functions:

Table 2-5. Dialog Box Icons

Icon	Function
Refresh	Refreshes the information in the table or dialog box. This clears any changes made to the table or dialog box and not yet sent to the device.
Apply	Sends the information from the table or dialog box to update the device.
Insert	Adds a row to the table.
Wizard	Starts a wizard.
Delete	Deletes the selected rows of the table.
Undo	Undoes all changes to the selected row in a table.

Using Avaya C360 Device Manager Help

This section explains how to use the on-line help in the Avaya C360 Device Manager. The on-line help can be opened to the contents page or directly to a topic of interest.

*** Note:** When running the Avaya C360 Manager via Web Management, on-line help is only available if you have installed the on-line help on your network and configured the Avaya C360 Device with the location of the help files. For information on installing the on-line help and configuring the device with the location of the files, refer to the *Avaya C360 User's Guide*.

Opening the Help to the Contents Page

To open the help to the contents page, select **Help > Contents**. The on-line help opens to the contents page.

Opening the Help to a Topic of Interest

To open the help directly to a topic of interest:

1. Click .

   Or

   Select **Help > Context Sensitive Help**. The cursor changes to the shape of an arrow with a question mark.

2. Click on a point of interest in the Avaya C360 Device Manager. The on-line help opens to a topic explaining the feature that was clicked.

3 Device Configuration

This chapter explains how to view and set the various configuration parameters relevant to the Avaya C360. It includes the following sections:

- **Viewing Device Information**- View high-level information about the Avaya C360 Device.
- **Viewing Module Configuration**- View information specific to an Avaya C360 module in the device.
- **Viewing LAG Configuration**- View information specific to a LAG on an Avaya C360 module in the device.
- **Viewing Port Configuration**- View information specific to the ports on the Avaya C360 Device.
- **Resetting the Device**- Reset the Avaya C360 Device.

To view configuration information, you must be in Configuration mode. To switch to Configuration mode:

Click .

Or

Select **View > Configuration**.

Viewing Device Information

The Device Information dialog box provides you with high-level information specific to the Avaya C360 Device.

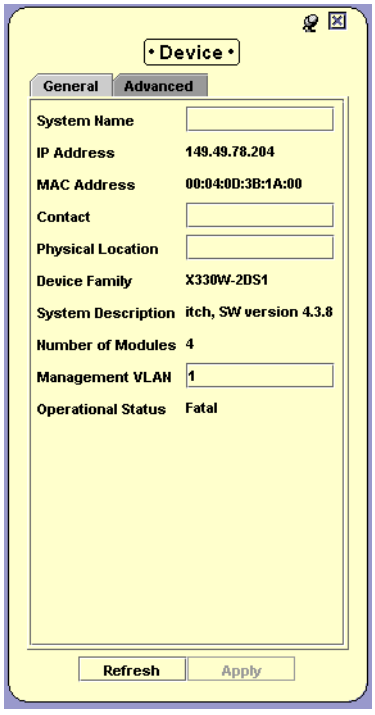
The General tab of the Device Information dialog box provides detailed information about the device such as the device's name, addresses, contact person, location, type, description, the number of modules in the device, and the management VLAN ID.

The Advanced tab of the Device Information dialog box provides information about the device's STP (Spanning Tree Protocol) configuration.

Device Information - General Tab

To view the General tab of the Device Information dialog box, select **Configure > Device Information**. The Device Information dialog box opens to the General tab.

Figure 3-1. Device Information Dialog Box - General Tab



The following table provides a list of the fields in the General tab of the Device Information dialog box and their descriptions.

Table 3-1. Device Information Fields - General Tab

Field	Description
System Name	Logical name of the device as defined on the SNMP agent of the device.
IP Address	The IP address of the device.
MAC Address	The MAC address of the device.
Contact	Individual responsible for maintenance of the device.
Physical Location	The current physical location of the device.
Device Family	The family of devices to which the device belongs.
System Description	A description of the device.
Number of Modules	The number of modules currently in the device.
Management VLAN	The VLAN ID (VLAN #) of the agent.
Operational Status	The warning level of the device. Possible values are: • **OK** • **Warning** • **Fatal**

For more information on the user interface, refer to "Using Dialog Boxes and Tables" on page 16.

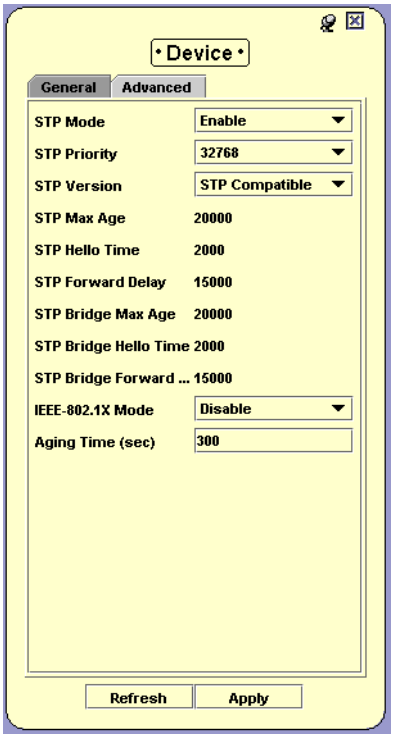
Device Information - Advanced Tab

To view the Advanced tab of the Device Information dialog box:

1. Select **Configure > Device Information**. The Device Information dialog box opens to the General tab.

2. Click **Advanced**. The Advanced tab of the Device Information dialog box appears.

Figure 3-2. Device Information Dialog Box - Advanced Tab



The following table provides a list of the fields in the Advanced tab of the Device Information dialog box and their descriptions.

Table 3-2. Device Information Fields - Advanced Tab

Field	Description
STP Mode	The state of Spanning Tree Protocol. Possible states are: • **Disable** - STP is disabled. This is the default state. • **Enable** - STP is enabled. When activating STP, keep in mind that: • All bridges should run STP. • Redundancy applications and STP cannot co-exist. For more information refer to *Spanning Tree Algorithm (STA)* in *The Reference Guide*.
STP Priority	The priority of the bridge as determined by the first quarter of the Bridge ID.

Table 3-2. Device Information Fields - Advanced Tab (Continued)

Field	Description
STP Version	The version of Spanning Tree Protocol to use. Possible versions include: • **Common Spanning Tree 802.1d** - The standard spanning tree protocol. • **rstp** - Rapid spanning tree protocol 802.1w.
STP Max Age	The maximum age of Spanning Tree Protocol information learned from the network on any port before it is discarded, in milliseconds. This is the actual value that this device is currently using.
STP Hello Time	The amount of time, in milliseconds, between the transmission of Configuration bridge PDUs by this node on any port when it is the root of the spanning tree or trying to become so. This is the actual value that this device is currently using.
STP Forward Delay	This speed, in milliseconds, at which a port changes its spanning state when moving towards the Forwarding state. The value determines how long the port stays in each of the Listening and Learning states, which precede the Forwarding state. This value is also used, when a topology change has been detected and is underway, to age all dynamic entries in the Forwarding Database.
STP Bridge Max Age	The maximum amount of time before Spanning recalculates if there is no change in network bridging status.
STP Bridge Hello Time	The amount of time between sending Spanning Tree updates if there are no detected changes in the overall bridged network topology.
STP Bridge Forward	The amount of time for the device to begin forwarding packets after recalculating its Spanning Tree table based on a change in network topology.

Table 3-2. Device Information Fields - Advanced Tab (Continued)

Field	Description
IEEE-802.1x Mode	The status of 802.1x authentication on the device. Possible values are: • **Enable** - Use 802.1x authentication for connections to this device. • **Disable** - Do not require authentication for connections to this device.
Aging Time (sec)	Amount of time MAC addresses remain in the CAM table.

For more information on the user interface, refer to "Using Dialog Boxes and Tables" on page 16.

Viewing Module Configuration

The Module Configuration dialog box provides you with information specific to a selected module.

The General tab of the Module Configuration dialog box provides detailed information about the module, such as the module's position in the device, the module's type, description, number of ports, mode of operation, and any faults occurring on the module.

The Advanced tab of the Module Configuration dialog box provides information about expansion, cascading, LLDP, and BUPS (BackUp Power Supply) modules that are connected to the selected module.

The Power tab of the Module Configuration dialog box provides information about the module's Power over Ethernet (PoE) configuration. For more information, refer to Chapter 4, *Power over Ethernet*.

If you have a G700 Media Gateway Module, the Module Configuration dialog box includes three additional tabs. For more information, refer to Chapter 5, *G700 Media Gateway*.

*** Note:** The information fields in the Module Configuration dialog box vary according to the type of module selected.

*** Note:** To view the configuration of an X330WAN expansion module, click the expansion module symbol in the Chassis View.

Module Configuration - General Tab

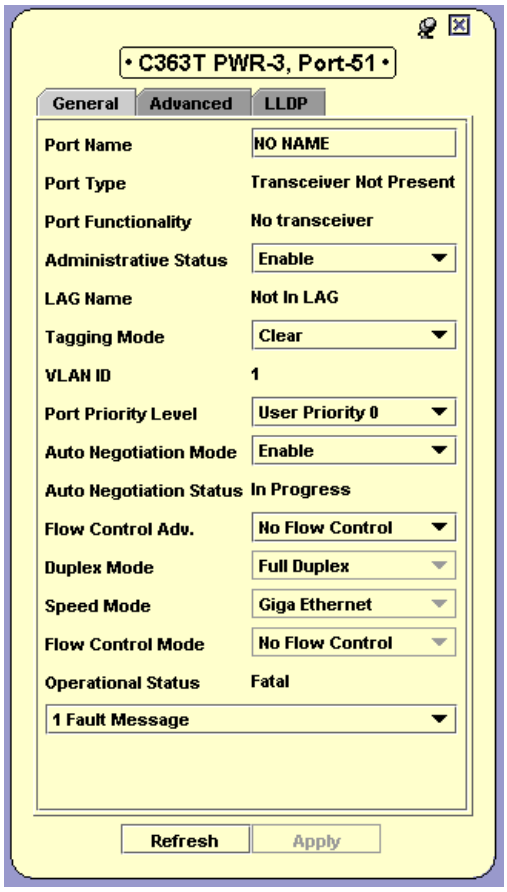
To view the General tab of the Module Configuration dialog box for a selected module:

Click the module symbol in the Tree View.

Or

Click the module's label in the Chassis View. The Module Configuration dialog box opens to the General tab.

Figure 3-3. Module Configuration Dialog Box - General Tab



The following table provides a list of the fields in the General tab of the Module Configuration dialog box and their descriptions:

Table 3-3. Module Configuration Fields - General Tab

Field	Description
Module ID	The position in which the module is located. There can be up to 10 modules in a device.

Table 3-3. Module Configuration Fields - General Tab (Continued)

Field	Description
Module Type	The module type. Possible values include: • **MM710** • **MM711** • **MM712** • **MM714** • **MM717** • **MM720** • **MM722** • **MM760** • **S8300**
Module Description	A description of the module type.
Number of Ports	The number of ports located on the module.
Software Version	The version of the application software running on the module.
Configuration Symbol	The version of the module. The version is updated whenever there is a functional modification to the module.
Serial Number	A unique number assigned by Avaya Inc. to the selected module.
Expansion Type	The type of expansion module in the selected module.
Expansion Description	A description of the expansion module in the selected module.
Expansion CS	The version of the expansion module. The version is updated whenever there is a functional modification to the module.
Cascading Type	The type of cascading module in the selected module. The cascading module is needed to connect modules in the device.
Cascading CS	The version of the cascading module. The version is updated whenever there is a functional modification to the module.

Table 3-3. Module Configuration Fields - General Tab (Continued)

Field	Description
Route Mode	The routing mode configured on a C360R module. Routing modes include: • **Second Layer** - The router module performs as a second layer module and performs no routing functions. • **Router** - The router module performs full routing functions.
Operational Status	The warning level of the module. Possible values are: • **OK** • **Warning** • **Fatal**
Fault Messages	A list of fault messages.

*** Note:** Media Modules cannot be inserted into the C360. Rather, they have to be inserted into G700, which is then stacked with the C360.

For more information on the user interface, refer to "Using Dialog Boxes and Tables" on page 16.

Module Configuration - Advanced Tab

To view the Advanced tab of the Module Configuration dialog box for a selected module:

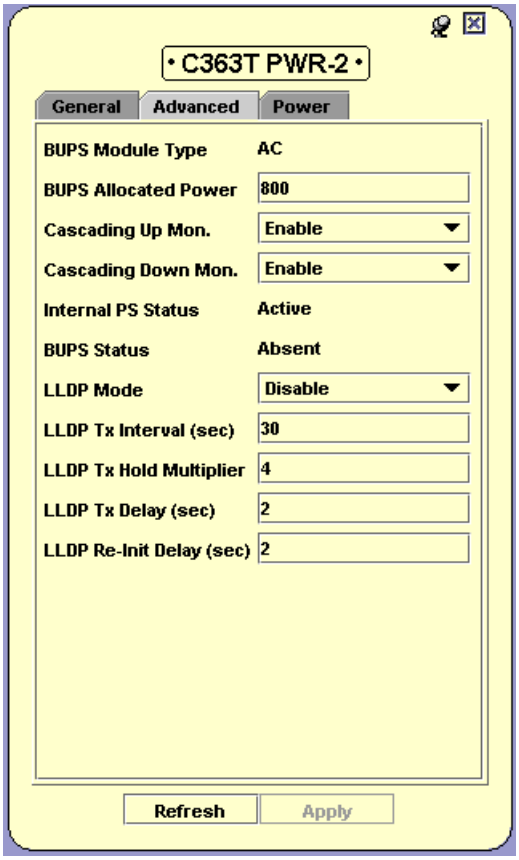
1. Click the module symbol in the Tree View.

   Or

   Click the module's label in the Chassis View. The Module Configuration dialog box opens to the General tab.

2. Click **Advanced**. The Advanced tab of the Module Configuration dialog box appears.

Figure 3-4. Module Configuration Dialog Box - Advanced Tab



The following table provides a list of the fields in the Advanced tab of the Module Configuration dialog box and their descriptions:

Table 3-4. Module Configuration Fields - Advanced Tab

Field	Description
BUPS Module Type	The type of BUPS (BackUp Power Supply) module in the selected module.
BUPS Module CS	The version of the BUPS (BackUp Power Supply) module. The version is updated whenever there is a functional modification to the module.
Cascading Up Mon.	Determines if the devices in the system are monitored cascading up. The possible values are: • **Enable** - Monitors devices in the network cascading up. If the connection is lost, the system reports a error. • **Disable** - Does not monitor devices in the network cascading up. If the connection is lost, the system does not report a error.
Cascade Down Mon.	Determines if the devices in the system are monitored cascading down. The possible values are: • **Enable** - Monitors devices in the network cascading down. If the connection is lost, the system reports a error. • **Disable** - Does not monitor devices in the network cascading down. If the connection is lost, the system does not report a error.
Internal PS Status	The operating status of the primary power supply.
BUPS Status	The operating status of the BUPS.
LLDP Mode	The status of Link Layer Discovery Protocol (LLDP) Mode on the device: • **Enable** - Use LLDP Mode. • **Disable** - Do not use LLDP Mode.
LLDP Tx Interval	The amount of time between packet transmissions on the device.

Table 3-4. Module Configuration Fields - Advanced Tab (Continued)

Field	Description
LLDP Tx Hold Multiplier	The LLDP time-to-live value expressed as a multiple of the value configured in the **LLDP Tx Interval** field.
LLDP Tx Delay	The delay between successive LLDP frame transmissions initiated by status changes in LLDP.
LLDP Re-Init Delay	The amount of time the device is instructed to wait before re-initiating LLDP.

For more information on the user interface, refer to "Using Dialog Boxes and Tables" on page 16.

Viewing LAG Configuration

The LAG Configuration dialog box provides you with information specific to a selected LAG.

The General tab of the LAG Configuration dialog box provides detailed information about the LAG, such as the LAG's status, name, VLAN tagging mode, VLAN ID, priority level, and mode of operation.

The Advanced tab of the LAG Configuration dialog box provides information about the LAG's STP configuration.

The Get/Set Toolbar provides an alternative, quick method to view and change a LAG's configuration. For more information on the Get/Set Toolbar, refer to "Get/Set Toolbar" on page 10.

LAG Configuration - General Tab

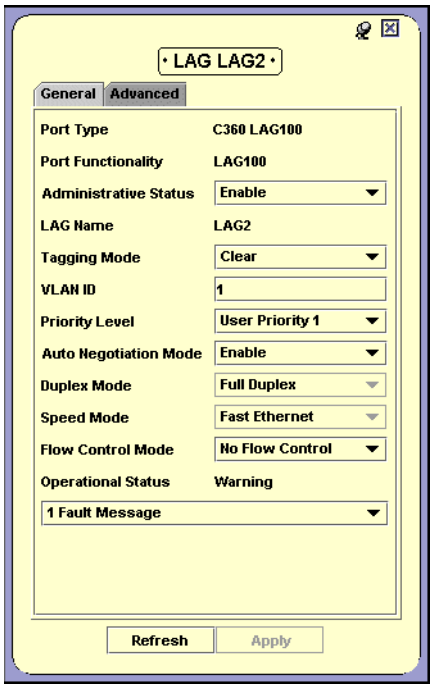
To view the General tab of the LAG Configuration dialog box for a selected LAG:

Click the LAG's symbol in the Tree View.

Or

Click the LAG's icon in the Chassis View. The LAG Configuration dialog box opens to the General tab.

Figure 3-5. LAG Configuration Dialog Box - General Tab



The following table provides a list of the fields in the General tab of the LAG Configuration dialog box and their descriptions:

Table 3-5. LAG Configuration Fields - General Tab

Field	Description
Port Type	The type of ports in the selected LAG.
Port Functionality	The physical media type of the ports of the selected LAG. If the port conforms to a certain standard (Repeater, Transceiver, 10BaseT, etc.), this standard is displayed. If the port does not conform to any standard, Private is displayed.

Table 3-5. LAG Configuration Fields - General Tab (Continued)

Field	Description
Administrative Status	The administrative state of the selected LAG: • **Enabled** - The LAG is enabled and can transmit and receive packets. • **Disabled** - The LAG is disabled and cannot transmit or receive packets.
LAG Name	The name of the LAG.
Tagging Mode	The LAG's operation mode regarding VLANs. The possible modes are: • **Clear** - Transmits each outgoing packet in untagged format if it belongs to the LAG's VLAN. Otherwise, it discards the packet. • **IEEE-802.1Q** - VLAN tagging, per IEEE 802.1Q VLAN standard. The LAG will transmit frames with a VLAN ID of 1 - 3071.
VLAN ID	The VLAN number of the LAG.
Priority Level	The priority level of packets exiting the LAG. For effective transmission, multimedia packets must be received isochronously (at regular intervals). To ensure this, you can assign priorities to packets coming out of a LAG. Whenever traffic load is extreme and a LAG cannot accept all incoming packets, packets sent from a LAG with the highest priority will pass through first. However, a fairness mechanism will allow low priority packets to eventually enter the bus. Possible values are **User Priority 0 .. User Priority 7**.

Table 3-5. LAG Configuration Fields - General Tab (Continued)

Field	Description
Auto Negotiation Mode	The configured state of the Auto-Negotiation protocol between two stations. When enabled, Auto-Negotiation detects the highest common denominator for communication between endstations, and sets both to the same highest common setting. It also delivers remote link status. For LAGs with 10BaseT and 100BaseT ports, Auto-Negotiation determines the speed and Duplex Mode of communication between the endstations. For LAGs with Gigabit ports, Auto-Negotiation determines the Flow Control setting of the ports. Possible values are: • **Enable** - Auto-Negotiation is enabled for this LAG. • **Disable** - Auto-Neotiation is not enabled for this LAG. For more information, refer to *Auto-Negotiation* in *The Reference Guide.*
Duplex Mode	The state of communication of the selected LAG. Possible values are: • **Full Duplex** - The LAG can send and receive simultaneously. • **Half Duplex** - The LAG can either receive or send, but can not do both simultaneously.
Speed Mode	The speed of communication of the ports on the selected LAG. Possible values are: • **Ethernet** - 10 Mbps. • **Fast Ethernet** - 100 Mbps. • **Gigabit Ethernet** - 1000 Mbps.
Flow Control Mode	The state of flow control on the selected LAG. Possible values are: • **No Flow Control** • **802.3x Sym**

Table 3-5. LAG Configuration Fields - General Tab (Continued)

Field	Description
Operational Status	The warning level of the ports on the selected LAG. Possible values are: • **OK** • **Warning** • **Fatal**
Fault Messages	A list of fault messages.

For more information on the user interface, refer to "Using Dialog Boxes and Tables" on page 16.

LAG Configuration - Advanced Tab

To view the Advanced tab of the LAG Configuration dialog box for a selected LAG:

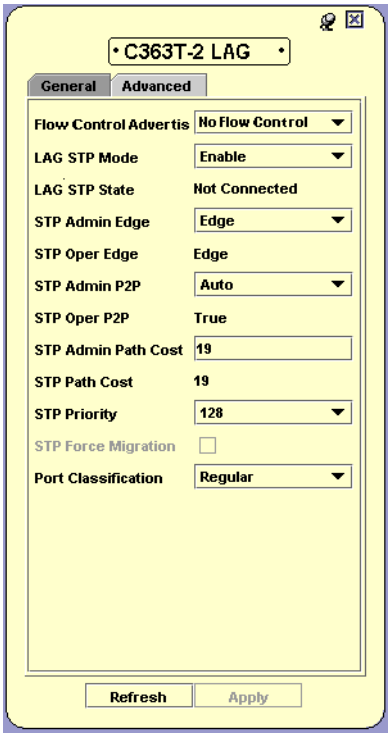
1. Click the LAG's symbol in the Tree View.

   Or

   Click the LAG's icon in the Chassis View. The LAG Configuration dialog box opens to the General tab.

2. Click **Advanced**. The Advanced tab of the LAG Configuration dialog box appears.

Figure 3-6. LAG Configuration Dialog Box - Advanced Tab



The following table provides a list of the fields in the Advanced tab of the LAG Configuration dialog box and their descriptions:

Table 3-6. LAG Configuration Fields - Advanced Tab

Field	Description
Flow Control Advertisement	The flow control values advertised by the LAGs on the selected LAG. These values limit the flow control possibilities to be decided by Auto-Negotiation.

Table 3-6. LAG Configuration Fields - Advanced Tab (Continued)

Field	Description
LAG STP Mode	Enables LAG Spanning Tree. The Spanning Tree mode creates a logical tree topology out of any arrangement of bridges, resulting in a single path between any two end stations. The Spanning Tree Mode also provides high fault tolerance. The possible states are: • **Enable** - Enables the Spanning Tree Mode. • **Disable** - Disables the Spanning Tree Mode. For more information refer to *Spanning Tree Algorithm (STA)* in *The Reference Guide*.
LAG STP State	The state of the LAG in terms of the Spanning Tree Protocol. The possible states are: • **Disable** - The LAG is disabled. • **Blocking** - STP is enabled and currently blocking the LAG. The LAG is effectively disabled to prevent the formation of a loop in the network. • **Forwarding** - The LAG is currently forwarding information received.
STP Admin Edge	The administrative state of the edge LAG parameter. Possible states include: • **TRUE** - This LAG is assumed to be an edge LAG. • **FALSE** - This LAG is assumed not to be an edge-LAG.
STP Oper Edge	The operational state of the edge LAG parameter. • **TRUE** - This LAG is operating in the state specified in STP Admin Edge. • **FALSE** - A BPDU was received by the LAG.

Table 3-6. LAG Configuration Fields - Advanced Tab (Continued)

Field	Description
STP Admin P2P	The administrative point-to-point status of the LAN segment attached to this LAG. Possible statuses include: • **True** - The LAG should always be treated as if it is connected to a point-to-point link. • **forceFalse** - The LAG should be treated as having a shared media connection. • **auto** - The LAG is considered to have a point-to-point link if it is an Aggregator and all of its members are aggregative, or if the MAC entity is configured for full duplex operation, either through auto-negotiation or by management means.
STP Oper P2P	The operational point-to-point status of the LAN segment attached to this LAG. It indicates whether a LAG is considered to have a point-to-point connection or not. The value is determined by STP Admin P2P.
STP Admin Path Cost	The administratively assigned value for the contribution of this LAG to the path cost of paths towards the spanning tree root. A value of 0 assigns the automatically calculated default Path Cost value to the LAG. STP Admin Path Cost complements STP Path Cost, which returns the operational value of the path cost.
STP Path Cost	The operational cost factor used by Spanning Tree Algorithm to determine the most efficient route for forwarding traffic to its destination while removing loops in the network. For more information refer to *Spanning Tree Algorithm (STA)* in *The Reference Guide*.
STP Force Migration	When checked and in RSTP mode, the LAG is forced to transmit RSTP BPDUs.

Table 3-6. LAG Configuration Fields - Advanced Tab (Continued)

Field	Description
Port Classification	The classification of a specific LAG. Port Classification allows network managers to specify each LAG level's importance. The possible states are: • **Regular** - Normal users. • **Valuable** - Servers or critical users. For more information refer to *Port Classification in The Reference Guide*.

For more information on the user interface, refer to "Using Dialog Boxes and Tables" on page 16.

Viewing Port Configuration

The Port Configuration dialog box contains tabs that provide you with information specific to a selected port.

The General tab of the Port Configuration dialog box provides detailed information about the port, such as the port name, type, functionality, status, VLAN ID, mode of operation, and any faults occurring on the port.

The Advanced tab of the Port Configuration dialog box provides detailed information about the port's STP configuration and port classification.

The 802.1x tab of the Port Configuration dialog box provides detailed information about the port's 802.1x configuration. For more information about 802.1x security, refer to Chapter 16, *Port Security*.

The Power tab of the Port Configuration dialog box provides information about the port's PoE configuration. For more information about PoE, refer to Chapter 4, *Power over Ethernet*.

The LLDP tab of the Port Configuration dialog box provides configuration information for the Link Layer Display Protocol on the port.

The Get/Set Toolbar provides an alternative, quick method to view and change the port's configuration. For more information on the Get/Set Toolbar, refer to "Get/Set Toolbar" on page 10.

*** Note:** The configuration of ports that participate in a LAG cannot be changed using the Port Configuration dialog box. Use the LAG Configuration dialog box instead.

*** Note:** The information fields in the Port Configuration dialog box vary according to the type of port selected.

Port Configuration - General Tab

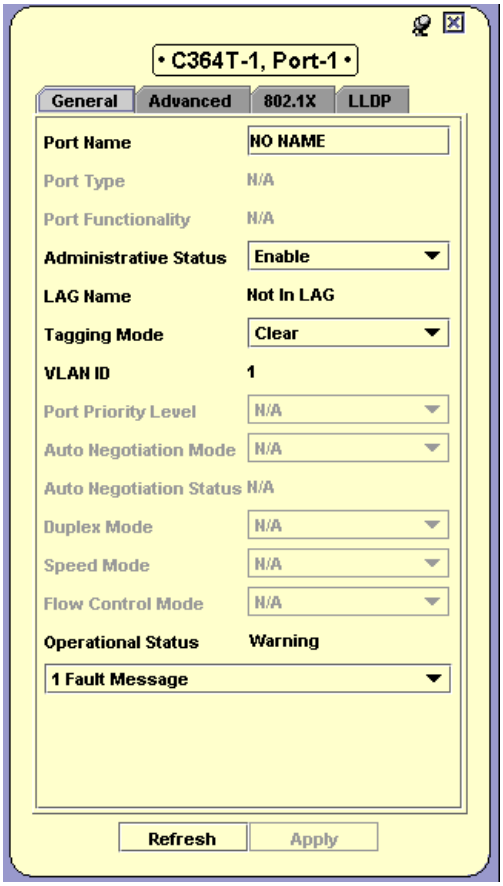
To view the General tab of the Port Configuration dialog box for a selected port:

Click the port symbol in the Chassis View.

Or

Click the port's icon in the Tree View. The Port Configuration dialog box opens to the General tab.

Figure 3-7. Port Configuration Dialog Box - General Tab



The following table provides a list of the fields in the General tab of the Port Configuration dialog box and their descriptions:

Table 3-7. Port Configuration Fields - General Tab

Field	Description
Port Name	The user can define a logical name to the port for ease of use.
Port Type	The port type; optionally includes reference to the module to which it is attached and port connector type.
Port Functionality	The physical media type of the selected port. If the port conforms to a certain standard (Repeater, Transceiver, 10BaseT, etc.), this standard is displayed. If the port does not conform to any standard, Private is displayed.
Administrative Status	The administrative state of the selected port: • **Enabled** - The port is enabled and can transmit and receive packets. • **Disabled** - The port is disabled and cannot transmit or receive packets.
LAG Name	The name of the LAG of which the port is a member. If the port is not a member of a LAG, the LAG Name is **not in LAG**.
Tagging Mode	The port's operation mode regarding VLANs. The possible modes are: • **Clear** - Transmits each outgoing packet in untagged format if it belongs to the port's VLAN. Otherwise, it discards the packet. • **802.1Q** - VLAN tagging, per IEEE 802.1Q VLAN standard. The port will transmit frames with a VLAN ID of 1 - 3071.
VLAN ID	The VLAN number of the port.

Table 3-7. Port Configuration Fields - General Tab (Continued)

Field	Description
Port Priority Level	The priority level of packets exiting the port or ports on the module. For effective transmission, multimedia packets must be received isochronously (at regular intervals). To ensure this, you can assign priorities to packets coming out of a port. Whenever traffic load is extreme and a port cannot accept all incoming packets, packets sent from a port with the highest priority will pass through first. However, a fairness mechanism will allow low priority packets to eventually enter the bus. Possible values are **User Priority 0 .. User Priority 7**.
Auto Negotiation Mode	The configured state of the Auto-Negotiation protocol between two stations. When enabled, Auto-Negotiation detects the highest common denominator for communication between endstations, and sets both to the same highest common setting. It also delivers remote link status. For 10BaseT and 100BaseT ports, Auto-Negotiation determines the speed and Duplex Mode of communication between the endstations. For Gigabit ports, Auto-Negotiation determines the Flow Control setting of the ports. Possible values are: • **Enable** - Auto-Negotiation is enabled on this port. • **Disable** - Auto-Negotiation is not enabled on this port. For more information, refer to *Auto-Negotiation* in *The Reference Guide.*

Table 3-7. Port Configuration Fields - General Tab (Continued)

Field	Description
Auto Negotiation Status	The operational state of the Auto-Negotiation protocol between two stations. Possible statuses are: • **Pass** - The Auto-Negotiation protocol is enabled and a common protocol has been established. • **In progress** - The Auto-Negotiation protocol is in the process of detecting the communication capabilities of the endstations and setting them to the highest common denominator. • **Fail** - The Auto-Negotiation protocol was not able to detect the communication capabilities of the end station, or was unable to set them to the highest common denominator. • **Disabled** - The Auto-Negotiation protocol is disabled.
Duplex Mode	The state of communication of the selected port. Possible values are: • **Full Duplex** - The port can send and receive simultaneously. • **Half Duplex** - The port can either receive or send, but can not do both simultaneously.
Speed Mode	The speed of communication of the selected port. Possible values are: • **Ethernet** - 10 Mbps. • **Fast Ethernet** - 100 Mbps. • **Gigabit Ethernet** - 1000 Mbps.
Flow Control Mode	The state of flow control on the selected port.
Operational Status	The warning level of the selected port. Possible values are: • **OK** • **Warning** • **Fatal**
Fault Messages	A list of fault messages.

For more information on the user interface, refer to "Using Dialog Boxes and Tables" on page 16.

Port Configuration - Advanced Tab

To view the Advanced tab of the Port Configuration dialog box for a selected port:

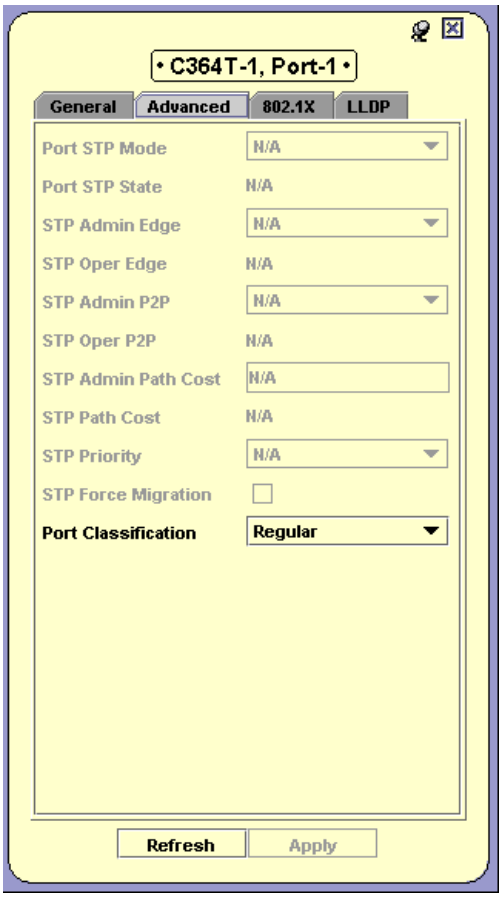
1. Click the port symbol in the Chassis View.

   Or

   Click the port's icon in the Tree View. The Port Configuration dialog box opens to the General tab.

2. Click **Advanced**. The Advanced tab of the Port Configuration dialog box appears.

Figure 3-8. Port Configuration Dialog Box - Advanced Tab



The following table provides a list of the fields in the Advanced tab of the Port Configuration dialog box and their descriptions:

Table 3-8. Port Configuration Fields - Advanced Tab

Field	Description
Port STP Mode	Enables Port Spanning Tree. The Spanning Tree mode creates a logical tree topology out of any arrangement of bridges, resulting in a single path between any two end stations. The Spanning Tree Mode also provides high fault tolerance. The possible states are: • **Enable** - Enables the Spanning Tree Mode. • **Disable** - Disables the Spanning Tree Mode. For more information refer to *Spanning Tree Algorithm (STA)* in *The Reference Guide*.
Port STP State	The state of the port in terms of the Spanning Tree Protocol. The possible states are: • **Disable** - The port is disabled. • **Blocking** - STP is enabled and currently blocking the port. The port is effectively disabled to prevent the formation of a loop in the network. • **Forwarding** - The port is currently forwarding information received.
STP Admin Edge	The administrative state of the edge port parameter. Possible states include: • **TRUE** - This port is assumed to be an edge port. • **FALSE** - This port is assumed not to be an edge-port.
STP Oper Edge	The operational state of the edge port parameter. • **TRUE** - This port is operating in the state specified in STP Admin Edge. • **FALSE** - A BPDU was received by the port.

Table 3-8. Port Configuration Fields - Advanced Tab (Continued)

Field	Description
STP Admin P2P	The administrative point-to-point status of the LAN segment attached to this port. Possible statuses include: • **True** - The port should always be treated as if it is connected to a point-to-point link. • **forceFalse** - The port should be treated as having a shared media connection. • **auto** - The port is considered to have a point-to-point link if it is an Aggregator and all of its members are aggregative, or if the MAC entity is configured for full duplex operation, either through auto-negotiation or by management means.
STP Oper P2P	The operational point-to-point status of the LAN segment attached to this port. It indicates whether a port is considered to have a point-to-point connection or not. The value is determined by STP Admin P2P.
STP Admin Path Cost	The administratively assigned value for the contribution of this port to the path cost of paths towards the spanning tree root. A value of 0 assigns the automatically calculated default Path Cost value to the port. STP Admin Path Cost complements STP Path Cost, which returns the operational value of the path cost.
STP Path Cost	The operational cost factor used by Spanning Tree Algorithm to determine the most efficient route for forwarding traffic to its destination while removing loops in the network. For more information refer to *Spanning Tree Algorithm (STA)* in *The Reference Guide*.
STP Priority	The priority factor used by STP to determine the activity status of an individual port on the Spanning Tree.
STP Force Migration	When checked and in RSTP mode, the port is forced to transmit RSTP BPDUs.

Table 3-8. Port Configuration Fields - Advanced Tab (Continued)

Field	Description
Port Classification	The classification of a specific port. Port Classification allows network managers to specify each port level's importance. The possible states are: • **Regular** - Normal users. • **Valuable** - Servers or critical users. For more information refer to *Port Classification in The Reference Guide*.

For more information on the user interface, refer to "Using Dialog Boxes and Tables" on page 16.

Port Configuration - LLDP Tab

Link Layer Discovery Protocol (LLDP) is a neighbor discovery protocol, which allows Ethernet network devices to search for, and request information from, other LLDP enabled devices on the network. LLDP defines a standard method for Ethernet network devices, such as switches, routers, and wireless LAN access points, to advertise information about themselves to other nodes on the network.

LLDP also allows Ethernet network devices to search for, and request information from, other devices using the LLDP protocol.

The following details can be advertised using LLDP on the Avaya C360 device:

- System Name
- Chassis ID
- Port ID
- System Description
- System Capabilities
- Port Description
- Management Address

*** Note:** Chassis ID and Port ID are always advertised when LLDP is enabled.

To view the LLDP tab of the Port Configuration dialog box for a selected port:

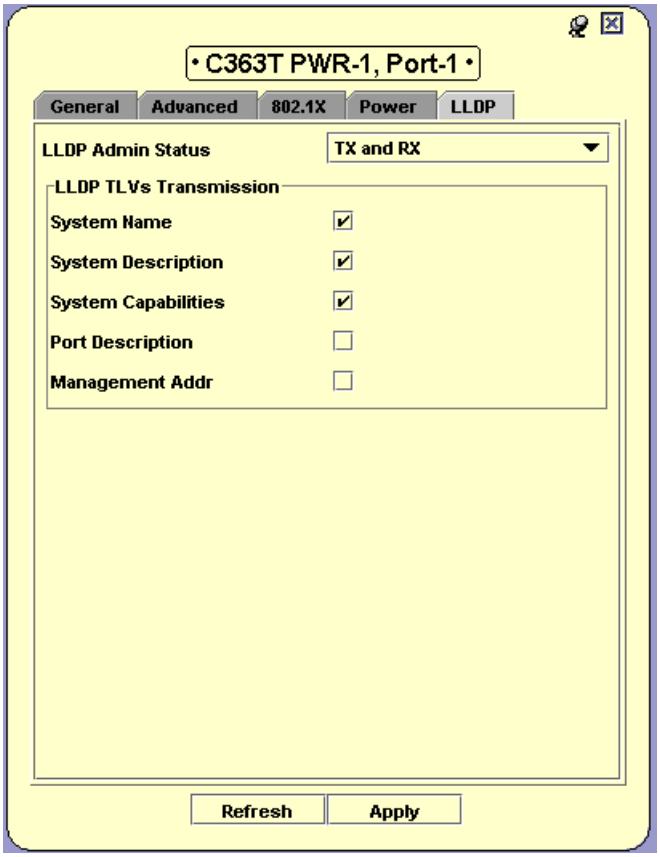
1. Click the port symbol in the Chassis View.

   Or

   Click the port's icon in the Tree View. The Port Configuration dialog box opens to the General tab.

2. Click the LLDP tab. The Port Configuration Dialog Box - LLDP Tab opens.

Figure 3-9. Port Configuration Dialog Box - LLDP Tab



The following table provides a list of the fields in the LLDP tab of the Port Configuration dialog box and their descriptions:

Table 3-9. Port Configuration Fields - LLDP Tab

Field	Description
LLDP Admin Status	The status of LLDP mode on the device. Possible values are: • **Tx Only** - LLDP mode is enabled, and is configured to only accept Tx traffic. • **Rx Only** - LLDP mode is enabled, and is configured to only accept Rx traffic. • **Tx and Rx** - LLDP mode is enabled, and is configured to accept both Tx and Rx traffic. • **Disabled** - LLDP mode is disabled. • **N/A** - LLDP mode is not supported for this port.
LLDP TLVs Transmission	The optional type length values advertised by the device. Possible values include: • **System Name**. • **System Description**. • **System Capabilities**. • **Port Description**. • **Management Address**. Selecting the checkbox instructs the device to advertise the indicated TLV. Leaving the checkbox blank instructs the device not to display the indicated TLV. **Chassis ID** and **Port ID** are not displayed as advertising their values is mandatory when LLDP is enabled.

Resetting the Device

You can reset the entire Avaya C360 Device, or one or more of its individual modules.

To reset the entire Avaya C360 Device:

1. Select **Action > Reset Device**. A confirmation dialog box opens.
2. Click **Yes**. The device resets.

To reset an individual Avaya C360 module:

1. Click the label of the module you want to reset.
   - To select multiple modules, press **CTRL** while clicking additional module labels.
2. Select **Actions > Reset Module(s)**. A confirmation dialog box opens.
3. Click **Yes**. The selected module resets.

To reset an individual G700 Media Module:

1. Click the label of the G700 Media Module you want to reset.
   - To select multiple modules, press **CTRL** while clicking additional module labels.
2. Select **Actions > Reset Media Module(s)**. A confirmation dialog box opens.
3. Click **Yes**. The selected module resets.

To reset an individual Avaya X330WAN module:

1. Click the label of the X330WAN module you want to reset.
   - To select multiple modules, press **CTRL** while clicking additional module labels.
2. Select **Actions > Reset WAN Plugin(s)**. A confirmation dialog box opens.
3. Click **Yes**. The selected module resets.

4 Power over Ethernet

This chapter provides information about Power over Ethernet (PoE) and includes the following sections:

- **PoE Overview** - An overview of Power over Ethernet functionality in Avaya C360 devices.
- **Viewing PoE Information** - Information about viewing PoE port information and configuring PoE on a module and port level.

PoE Overview

PoE provides power to IP telephones over an Ethernet line using an Avaya C360 device. The power is transmitted via the device's ports to the IP telephones over the same cable carrying IP packets.

The Avaya C360 device automatically discovers the connection and removal of IP telephones from the in-line powered ports and provides power accordingly.

The Avaya C360 provides the power using an internal 225 watt power supply over a 48 volt feed. It is possible to attach an external power supply either for additional power, or as an alternative power supply should the internal power supply fail.

In addition, you can configure power priorities per port ensuring that important equipment is guaranteed power whenever necessary.

Viewing PoE Information

This section provides information about viewing port information and configuring PoE on the port and module level, and includes the following:

- **Viewing PoE Port Information**
- **Viewing PoE Configuration**

Viewing PoE Port Information

The Chassis View provides immediate information about PoE. Ports that are currently supplying power to IP telephones are labeled with a lightning bolt.

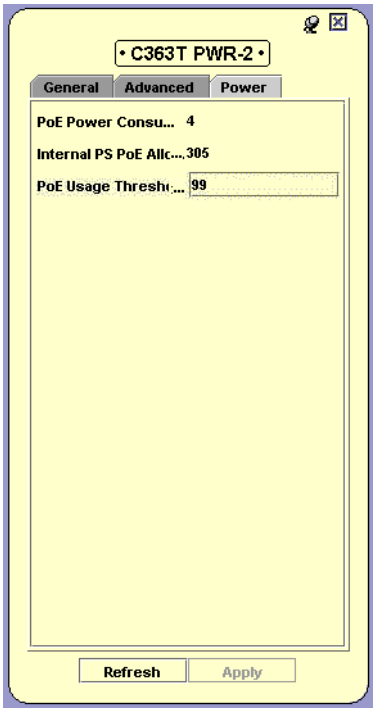
Viewing PoE Configuration

You can view PoE configuration information on the module and port levels.

PoE Module Configuration

To view the PoE configuration on a module that supports PoE, select the Power tab in the module's configuration dialog box. For information on opening the Module Configuration dialog box, refer to "Viewing Module Configuration" on page 24.

Figure 4-1. Module Configuration - Power Tab



The following table provides a list of the fields in the Power tab of the Module Configuration dialog box and their descriptions:

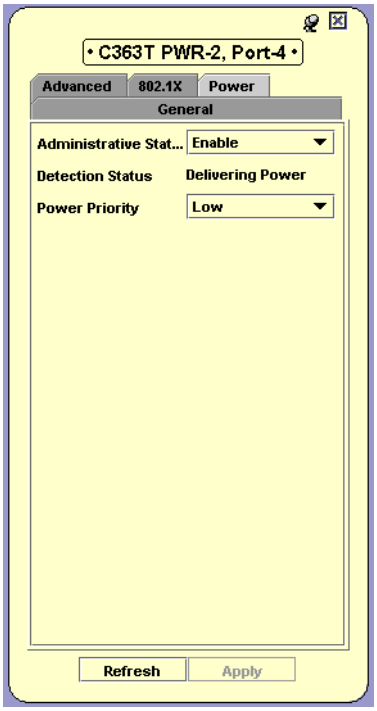
Table 4-1. Module Configuration - Power Fields

Field	Description
PoE Power Consumption [W]	The current power consumption of the devices attached to the module.
Internal PS PoE Allocation[W}	The total available power output that can be allocated by the module's internal power supply (in Watts).
PoE Power Threshold [%]	The percentage of available allocated power being used by the module.

PoE Port Configuration

To view the PoE configuration on a port that supports PoE, select the Power tab in the port's configuration dialog box. For more information on opening the Port Configuration dialog box, refer to "Viewing Port Configuration" on page 39.

Figure 4-2. Port Configuration - Power Tab



The following table provides a list of the fields in the Power tab of the Module Configuration dialog box and their descriptions:

Table 4-2. Port Configuration - Power Fields

Field	Description
Administrative Status	The administrative state of power on this port. Possible states include: • **Enable** - This port can supply power to IP telephones. • **Disable** - This port cannot supply power to IP telephones.

Table 4-2. Port Configuration - Power Fields (Continued)

Field	Description
Detection Status	The operational state of power on this port. Possible states include: • **Searching** - Port is currently being polled. • **Delivering Power**- This port is supplying power to an IP telephone. • **Failed** - This port is currently not supplying power to an IP telephone.
Power Priority	The priority of the power being supplied by this port. When the demand for power exceeds the modules capacity, ports with lower priority will be prevented from supplying power before ports with a higher priority. Possible priorities include: • **Critical** • **High** • **Low**

5 G700 Media Gateway

This chapter provides information about the Avaya G700 Media Gateway and includes the following sections:

- **G700 Media Gateway Overview** - An overview of G700 functionality in Avaya C360 Devices.
- **G700 Configuration**- Information about viewing and configuring G700 components.
- **Avaya Site Administration** - Information about Avaya's gatekeeper software.

G700 Media Gateway Overview

G700 is a family of components which can deliver data, voice, fax, and messaging capabilities over an IP network.

The heart of the G700 system is the Media Gateway. The Media Gateway is a VoIP system that acts as an IP PBX and messaging server and a VoIP gateway. In addition, it performs the function of a gatekeeper and an IP media management resource for tone detection and generation, conferencing, and call classification.

The Media Gateway components are controlled through the Media Gateway Processor (MGP). The MGP detects when a media module is inserted or removed and transfers information from the VoIP engine to the other components.

G700 converges the power of Avaya Call Processing (ACP) software with the power of distributed switching from the Avaya C360 Device. It provides IP PBX functionality using open standards and an open operating system. The G700 device connects to ACP using either an internal or external call controller. The ACP serves as the G700's gatekeeper.

G700 Configuration

This section describes how to view and set the various configuration parameters relevant to the G700 Media Gateway. It includes the following sections:

- **Viewing Module Configuration**- View information specific to a G700 Media Gateway module in the device.
- **Viewing Media Module Configuration**- View information specific to a Media Module in the device.

Viewing Module Configuration

The Module Configuration dialog box provides you with information about a selected module. To view the configuration of a module:

Click the module symbol in the Tree View.

Or

Click the module's label in the Chassis View. The Module Configuration dialog box opens.

The Module Configuration dialog box for G700 modules contains four tabs:

- **Switch Config**
- **MG Config**
- **MGP Config**
- **MGC Config**

*** Note:** For information about configuring Avaya C360 Modules other than the G700 Media Gateway, refer to "Viewing Module Configuration" on page 24.

Switch Config

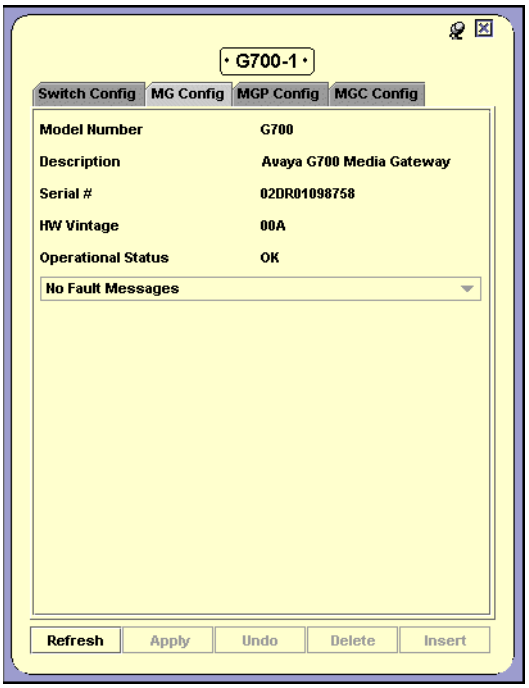
The Switch Config tab provides detailed information about the module, such as the module's position in the device, the module's type, description, number of ports, and any faults occurring on the module.

For information about the fields in the Switch tab, refer to "Viewing Module Configuration" on page 24.

MG Config

The MG Config tab provides information about the Media Gateway's hardware configuration and operational status.

Figure 5-1. MG Config Tab



The following table lists the fields in the MG Config tab of the Module Configuration dialog box and their descriptions.

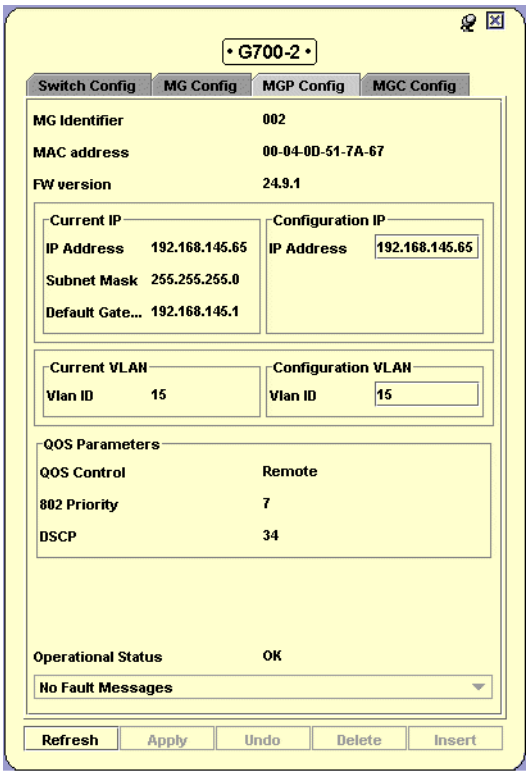
Table 5-1. MG Config Parameters

Field	Description
Model Number	The model number of the media gateway.
Description	A description of the gateway.
Serial #	The serial number of the gateway.
HW Vintage	The hardware vintage version of the gateway.
Operational Status	The operational status of the media gateway.

MGP Config

The MGP Config tab provides hardware information about the Media Gateway Processor. In addition, the MGP Config tab is used to configure IP, VLAN, and QoS parameters.

Figure 5-2. MGP Config Tab



General

The upper section of the MGP Config tab provides general information about a specific Media Gateway Processor.

The following table lists the General fields and their description.

Table 5-2. MGP Config Tab - General Parameters

Field	Description
MG Identifier	The ID of the MG that helps link the C360 module's port identification with the G700 Media Gateway's port identification.
MAC address	The MAC address of the media gateway processor.
FW version	The firmware version of the media gateway processor.

IP Address Settings

You can manually configure the IP address settings for the Media Gateway. The Current IP box displays the IP address configuration currently being used. The information in the Current IP box is Read-only. The Configuration IP box displays the IP configuration.

The following table lists the IP address settings fields and their descriptions.

Table 5-3. MGP Config - IP Address Settings Parameters

Field	Description
IP Address	The IP address of the gateway processor.
Subnet Mask	The subnet mask of the gateway processor. When Use DHCP for IP is unchecked, the Subnet Mask is configured using the CLI. For more information on CLI commands, refer to the *Avaya C360 User's Guide*.
Default Gateway	The default gateway of the gateway processor. When Use DHCP for IP is unchecked, the Gateway is configured using the CLI. For more information on CLI commands, refer to the *Avaya C360 User's Guide*.

VLAN Settings

You can manually configure the VLAN to which the G700 Media Gateway belongs. The Current VLAN field displays the actual ID that you are using. The information is taken from the Configuration VLAN field.

The following table lists the VLAN settings fields and their descriptions.

Table 5-4. MGP Config - VLAN Settings Parameters

Field	Description
VLAN ID	The VLAN ID of the gateway.

QoS Parameters

QoS can be controlled either locally or remotely. If control is remote, the information for these fields comes from the gatekeeper. If control is local, you can configure the 802 Priority and DSCP fields.

The following table lists the QoS parameters and their descriptions.

Table 5-5. MGP Config - QoS Parameters

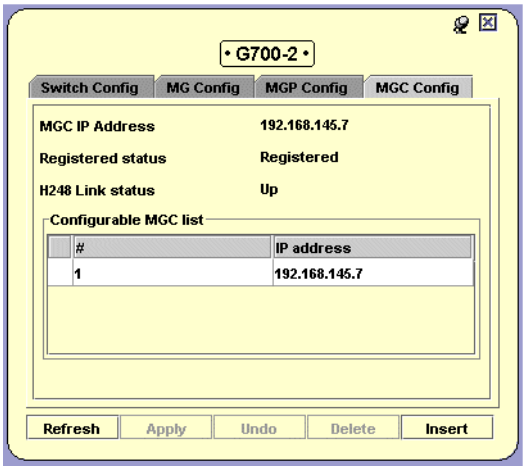
Field	Description
QoS Control	The source of QoS control. This parameter can only be changed via the CLI. Possible values are: • **Local** - The processor is using the local QoS parameters. The 802 Priority and DSCP fields can be configured. • **Remote** - The processor is receiving QoS parameters from the Media Gateway Processor. All QoS parameters are Read-only.
802 Priority	Priority based on a 802.1p standard, which assigns rights and privileges to users of a telephony network. Possible values are 0 - 7.
DSCP	Priority based on a technology by which packets are marked in the IP header Type of Service (ToS) byte as belonging to a certain class. Possible values range are 0 - 63.

In addition, the operational status of the MGP and any faults on the MGP appear at the bottom of the MGP Config tab.

MGC Config

The MGC Config tab provides information about the Media Gateway Controller's settings, IP address, and registration information.

Figure 5-3. MGC Config Tab



MGC IP Settings

The MGC registers with the Media Gateway, after which it receives its IP address from the Media Gateway. After you register, the Link Status will be Up, and an IP address will appear.

The following table lists the MGC IP Settings fields and their descriptions.

Table 5-6. MGC Config - MGC IP Settings Parameters

Field	Description
MGC IP Address	The IP address of the call controller serving the media gateway.
Registered status	Shows whether this media gateway is currently registered with any call controller.
H248 Link Status	Status of the link connecting the media gateway to the active call controller.

MGC Lists

The MGC List provides a list of controllers. If the MGP is unable to establish a connection with the first controller in the list, the MGP will try to establish a connection with the next controller in the list. This process continues until a connection is established with one of the controllers.

You can manually configure the MGC list or you can get the MGC list from the DHCP server.

To add an entry to the Configurable MGC list:

1. Click **Insert**. A new row appears.
2. Enter the IP address for the entry. The new entry is created.

   The MGCs are registered in the order that they appear in the MGC list.

To modify an entry in the Configurable MGC list, modify the information in the entry's row in the table.

To delete an entry from the Configurable MGC list:

1. Select the entry in the list.
2. Click **Delete**. The entry is deleted.

   — To select more than one entry, press **SHIFT** while selecting additional entries.

*** Note:** To apply the changes to the MGC list, click **Apply**.

Viewing Media Module Configuration

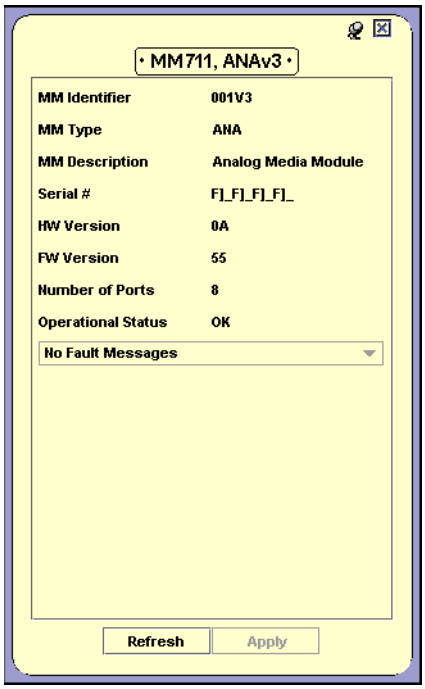
To view the Media Module Configuration dialog box:

In Configuration Mode, click the media module symbol in the Tree View.

Or

Click the media module's label in the Chassis View. The Media Module Configuration dialog box opens.

Figure 5-4. Media Module Configuration Dialog Box



The Media Module Configuration dialog box provides information about a specific media module, including a brief description of the media module, the number of ports, and its operational status.

The following table lists the fields in the Media Module Configuration dialog box and their description.

Table 5-7. Media Module Configuration Parameters

Field	Description
MM Identifier	The Media Module's identifier.
MM Type	The type of Media Module. Possible values are: • E1/T1 • ISDN BRI • Analog • Digital • VoIP • ICC
MM Description	An optional description of the specific Media Module.
Serial #	The serial number of the Media Module.
HW Version	The version of the Media Module's hardware.
FW Version	The firmware version of the Media Module.
Number of Ports	The number of ports on the Media Module.
Operational Status	The operational status of the Media Module.

Avaya Site Administration

Avaya Site Administration (ASA) is an administration tool for Avaya Call Processing call control software. ASA is used to configure the current MGC, G700 Media Gateway, or an individual voice port.

To launch ASA on an MGC, G700 Media Gateway, or voice port:

1. Click the component in the Tree View or Chassis View.
2. Click .

   Or

   Select **Tools > Administer Station/Gateway**. ASA opens with the configuration form of the selected component.

If you have a registered call controller MM installed in your G700 Media Gateway, you can launch ASA on the call controller. To launch ASA on a registered call controller media module:

1. Select the registered call controller media module.
2. Select **Tools > Administer Call Controller**. ASA opens on the selected call controller.

For more information about ASA, refer to Definity Enterprise Management documentation.

6 VoIP Engine Configuration

This chapter provides information and instructions for viewing and configuring the VoIP Engine features. It includes the following sections:

- **VoIP Overview** - An overview of VoIP Engine functionality in G700 Media Gateway modules.
- **Configuring the VoIP Engine**- Instructions for viewing and configuring VoIP Engine parameters.

VoIP Overview

The VoIP Engine translates information between different VoIP and data protocols. The G700 device manager comes with an internal VoIP engine that supports up to 32 simultaneous sessions. Support for an additional 32 simultaneous sessions can be added by inserting a VoIP Media Module in the G700 Media Gateway Module.

Configuring the VoIP Engine

You can view information and configure parameters for the VoIP Engine using the VoIP Engine dialog box. To view the VoIP Engine dialog box:

1. Select a G700 Media Gateway module.
2. Select **Configure > MediaGateway > VoIP Configuration**. The VoIP Engine dialog box opens.

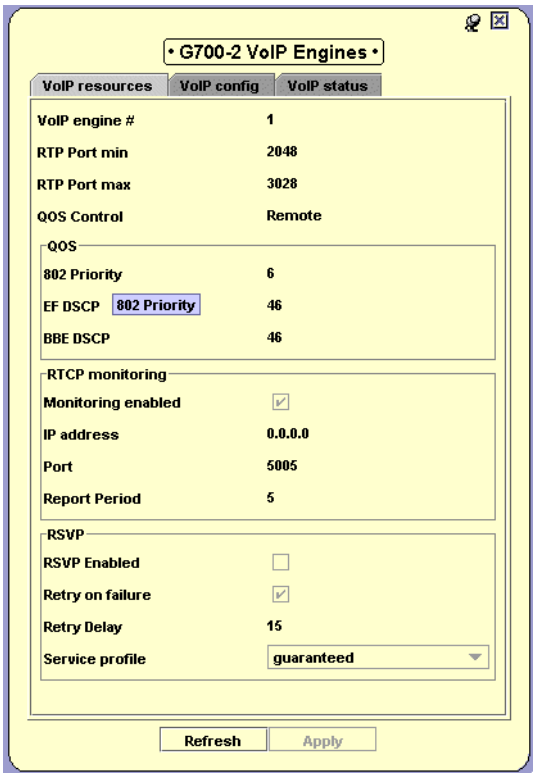
The VoIP Configuration dialog box contains three tabs:

- **VoIP Resources**
- **VoIP Config**
- **VoIP Status**

VoIP Resources

The VoIP resources tab provides administration parameters common to all VoIP engines, such as the number of engines, QoS parameters, RTCP configuration, and RSVP configuration.

Figure 6-1. VoIP resources Tab



General

The upper section of this dialog box displays general information common to all VoIP engines.

The following table lists the general fields in the VoIP resources tab of the VoIP Engine dialog box and their description.

Table 6-1. VoIP resources - General Parameters

Field	Description
VoIP Engine #	The number of VoIP engines in the media gateway.
RTP port Min	The minimum range of UDP ports assigned by the call controller for RTP traffic. The value ranges between 1 - 65534.

Table 6-1. VoIP resources - General Parameters (Continued)

Field	Description
RTP port Max	The maximum range of UDP ports assigned by the call controller for RTP traffic. The value ranges between 3 - 65535.

QoS

QoS can be controlled either locally or remotely. If control is local, it is possible to configure QoS, RTCP, and RSVP parameters. If control is remote, QoS parameters are determined by the MGC.

The following table lists the QoS fields and their descriptions.

Table 6-2. VoIP resources - QoS Parameters

Field	Description
QoS Control	The source of QoS control. This parameter can only be changed via the CLI. Possible values are: • **Local** - The processor uses the local QoS parameters. If the processor is using the local QoS parameters, the 802 Priority, EF DSCP, and BBE DSCP fields can be configured. • **Remote** - The processor receives its QoS parameters from the Media Gateway Controller. All QoS parameters are Read-only.
802 Priority	Priority based on a CoS standard which assigns rights and privileges to users of a telephony network. Possible values are 0 - 7.
EF DSCP	A type of differentiated service used to provide guaranteed bandwidth across a network. If sufficient bandwidth is available, the Expedited Forwarding class can be used. The values range are 0 - 63.
BBE DSCP	A DiffServ class which is used per call to achieve the greatest possible bandwidth. The values range between 0 - 63.

RTCP Monitoring

RTCP is an IP protocol that is used to monitor the quality of RTP packets. Quality is measured in terms of delay, jitter, and packet loss.

If RTCP monitoring is enabled, the VoIP engines send RTCP packets to the RTCP monitor. You must configure an IP address for the RTCP monitor, and determine intervals at which the RTCP data is checked.

The following table lists the RTCP monitoring fields and their descriptions.

Table 6-3. VoIP resources - RTCP monitoring Parameters

Field	Description
Monitoring Enabled	The status of RTCP monitoring. • **Checked** - RTCP monitoring is enabled. • **Unchecked** - RTCP monitoring is disabled.
IP address	The IP address of the RTCP monitor.
Port	The port monitored by RTCP.
Report Period	The interval for RTCP reports.

RSVP

RSVP is a protocol that signals the router to reserve bandwidth.

If RSVP is enabled, the G700 Media Gateway tries to reserve a specific amount of bandwidth per call session. If this fails, the Media Gateway tries to reallocate the bandwidth during the call session.

The following table lists the RSVP fields and their description.

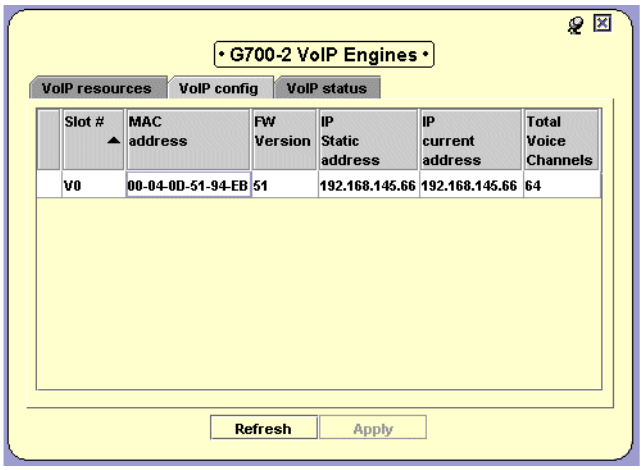
Table 6-4. VoIP resources - RSVP Parameters

Field	Description
RSVP Enabled	The Status of RSVP usage. • **Checked** - The G700 Media Gateway will try to reserve bandwidth per call. If it fails, the G700 Media Gateway will try again during the call. • **Unchecked** - RSVP is not enabled.
Retry on failure	The action the VoIP engine takes after an RSVP request fails. • **Checked** - The VoIP engine resends a RSVP request if the first attempt failed. • **Unchecked** - The VoIP Engine drops the RSVP request, and the Retry Delay field is ignored.
Retry Delay	The interval the VoIP Engine waits after a failed RSVP request before sending the new request. The interval ranges between 0.5 - 60 seconds.
Service profile	The type of service being provided.

VoIP Config

The VoIP config tab allows you to view information about a specific VoIP engine's configuration.

Figure 6-2. VoIP config Tab



You can configure the IP address to be used in the IP Static Address field. In addition, it is possible to see how many VoIP channels are available on this engine.

The information in the VoIP config tab is provided by the VoIP engine and is refreshed periodically.

The following table lists the fields in the VoIP config tab and their description.

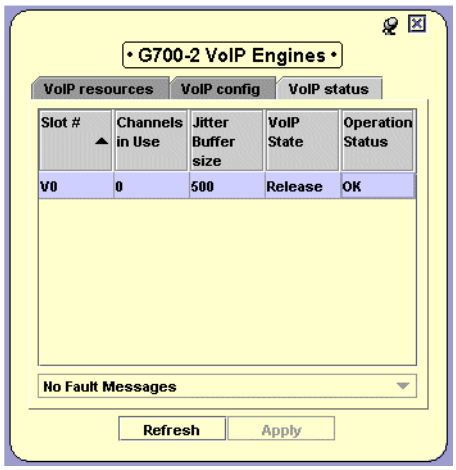
Table 6-5. VoIP config Parameters

Field	Description
Slot #	The slot in which the VoIP media module engine is located.
MAC address	The MAC address of the VoIP engine.
FW Version	The firmware version on the VoIP engine.
IP Static address	The IP address assigned to the VoIP Engine when not using the DHCP server.
IP current address	The current IP address of the VoIP engine.
Total Voice Channels	Total number of channels available for this VoIP engine.

VoIP Status

The VoIP status tab provides information about a specific engine's operational status, jitter buffer size, and number of sessions open.

Figure 6-3. VoIP status Tab



The information in the VoIP status tab is provided by the VoIP engine and is refreshed periodically.

The following table lists the fields in the VoIP status tab and their descriptions.

Table 6-6. VoIP status Parameters

Field	Description
Slot #	The slot in which the VoIP engine is located.
Channels in Use	The number of channels currently being used.
Jitter Buffer Size	The jitter buffer is a temporary storage area built into the receiver of each gateway. It uses a mechanism to remove the random delays between packets, which occur as the packets are routed through the network.
VoIP State	The state of the VoIP engine.
Operational Status	The operational status of the VoIP engine.
Fault Messages	Fault messages for the VoIP engine.

7 WAN Configuration

This chapter provides information about configuring Avaya X330WAN Expansion Modules and includes the following sections:

- **X330WAN Overview** - An overview of X330WAN functionality in Avaya C360 Devices.
- **Avaya X330WAN Expansion Module Configuration** - Information about viewing and configuring the X330WAN Expansion Module.
- **E1/T1 Port Configuration** - Information about viewing and configuring the E1/T1 ports on an X330WAN Expansion Module.
- **Viewing Channel Group Information** - Information about viewing and configuring channel groups on E1/T1 ports.
- **Managing Channel Groups** - Information about managing channel groups on E1/T1 ports.
- **USP Configuration** - Information about viewing and configuring the Universal Serial ports (USPs) on an X330WAN Expansion Module.
- **Backup Interface Configuration** - Information about viewing and configuring Backup interfaces.

For information on configuring the X330WAN's Ethernet ports, refer to "Viewing Port Configuration" on page 39.

X330WAN Overview

The X330WAN is a WAN expansion module that can be inserted into modules of the Avaya C360 line that include an expansion slot.

The X330WAN Expansion Module adds WAN connectivity to the Avaya C360 stackable line. WAN connectivity provides a link to the WAN enabling heavy data transfer over long distances. A WAN connection can connect branch offices to headquarters. In addition, WAN connectivity is essential for providing access to the Internet.

Avaya X330WAN Expansion Module Configuration

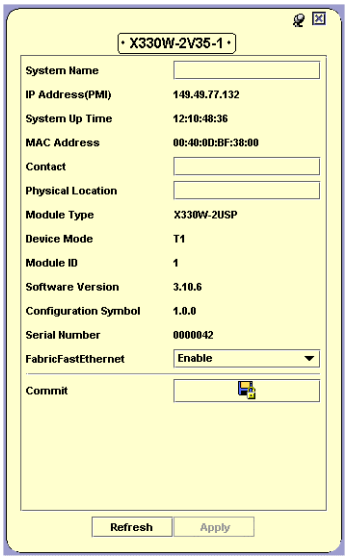
The X330WAN Expansion Module configuration dialog box provides you with information specific to a selected WAN expansion module. To view the configuration of an expansion module:

Click the expansion module symbol in the Tree View.

Or

Click the expansion module's label in the Chassis View. The Expansion Module dialog box opens.

Figure 7-1. Expansion Module Dialog Box



The Expansion Module dialog box provides detailed information about the module, such as the module's name, IP address, location, description and serial number.

For information about the fields in the Expansion Module dialog box, refer to "Viewing Module Configuration" on page 24.

To apply changes to the X330WAN module configuration, click **Apply**.

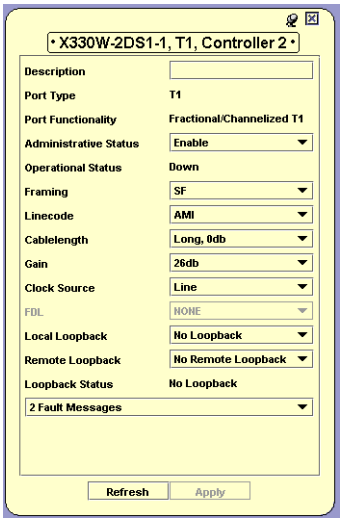
To save the changes to the X330WAN module configuration to the startup configuration, click . The configuration changes are saved.

E1/T1 Port Configuration

In addition to the Ethernet ports found on an Avaya C360 device, the X330WAN expansion module may have E1/T1 ports. This section provides information on viewing and configuring E1/T1 port parameters.

To display the E1/T1 Port Configuration dialog box, click the E1/T1 port's symbol in the Chassis View or the Tree View. The E1/T1 Port Configuration dialog box opens.

Figure 7-2. E1/T1 Port Configuration Dialog Box



The E1/T1 port is used to connect to an E1 or T1 line. The E1/T1 Port Configuration dialog box provides configuration and status information about the E1/T1 port.

The following table lists the E1/T1 Port Configuration fields and their descriptions:

Table 7-1. E1/T1 Port Configuration Parameters

Field	Description
Description	The E1/T1 port description.
Port Type	The type of E1/T1 port. Possible values are: • **E1** - For E1 and ISDN lines with 32 available channels. • **T1** - For T1 lines with 24 available channels.
Port Functionality	The type of E1 or T1 line.
Administrative Status	The state of the selected port. Possible values are: • **Enabled** - The port is enabled and can transmit and receive packets. • **Disabled** - The port is disabled and cannot transmit or receive packets.
Operational Status	The operational status of the port.
Framing	The type of framing. For an E1 line: • **CRC4** • **no-CRC4** • **Unframed** *** Note:** If **Unframed** is selected, all channels are used for an unframed Channel Group, and the Advanced tab does not appear in the Channel Group dialog box. For a T1 line: • **ESF** • **SF**

Table 7-1. E1/T1 Port Configuration Parameters (Continued)

Field	Description
Linecode	The type of linecode. Possible values are: For an E1 line: • **HDB3** • **AMI** For a T1 line: • **B8ZS** • **AMI**
Cablelength (T1 only)	The recommended maximum cable length.
Gain (T1 only)	The gain on this interface.
Clock Source	The source of the Transmit Clock. Possible sources include: • **Line** - The recovered receive clock is used as the transmit clock. • **Internal** - The local clock is used as the transmit clock.
FDL (T1 only)	The type of FDL used on this interface. Possible types include: • **ANSI** • **AT&T** • **Both** - ANSI and AT&T FDl are both used on this interface.
Local Loopback	A request to use a local loopback. A local loopback can be performed using: • **No Loopback** • **Payload Loopback** • **Line Loopback** • **Diag Loopback**
Remote Loopback (T1 only)	A request to use a remote loopback. A remote loopback can be performed using: • **No Remote Loopback** • **Remote Line** • **Remote Payload**

Table 7-1. E1/T1 Port Configuration Parameters (Continued)

Field	Description
Loopback status	The type of loopback currently used by the port. Possible values are: • **Near End Payload** • **Near End Line** • **Near End Inward** • **Far End Payload** • **Far End Line**
Fault Messages	Any faults that occurred on the port.

Viewing Channel Group Information

The Channel Group dialog box contains provide information specific to a selected Channel Group. The tabs that appear in the Channel Group dialog box are dependant on the encapsulation method of the selected Channel Group.

To view the Channel Group dialog box for a specific Channel Group:

1. Click a Channel Group symbol in the Chassis View. A list of Channel Groups appears.
2. Click the Channel Group for which you want to view information. The Channel Group dialog box for the selected Channel Group opens.

*** Note:** Clicking **New** opens the Channel Group wizard, enabling creation of a new Channel Group on the selected port. For information about the Channel Group Wizard, refer to "The Channel Group Wizard" on page 101.

Channel Group - PPP Session Information

The Channel Group dialog box for Channel Groups using PPP Sessions contains three tabs:

- **Channel Group** - Basic information about the Channel Group.
- **Advanced** - Information about the channels that comprise the Channel Group.
- **PPP** - Information about PPP on the Channel Group.

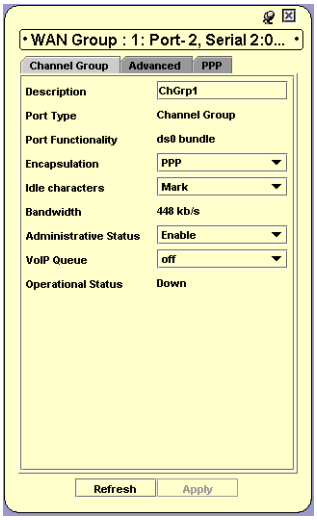
Channel Group

The Channel Group tab of the Channel Group dialog box provides basic information about the selected Channel Group.

To view the Channel Group tab of the Channel Group dialog box:

1. Click a Channel Group icon in the Chassis View. A list of Channel Groups on the port appears.
2. Click the Channel Group you want to configure. The Channel Group dialog box opens with the Channel Group tab.

Figure 7-3. Channel Group Dialog Box - Channel Group Tab



The following table provides a list of the fields in the Channel Group tab of the Channel Group dialog box and their descriptions:

Table 7-2. Channel Group Dialog Box - Channel Group Parameters

Field	Description
Description	A description of the PPP session.
Port Type	The port type.
Port Functionality	The framing mode of the port. Possible modes are: • **ds0 bundle** • **Unframed E1** (for E1 ports only)

Table 7-2. Channel Group Dialog Box - Channel Group Parameters (Continued)

Field	Description
Encapsulation	The encapsulation method for the PPP session. Possible encapsulation types are: • **PPP** • **Frame Relay**
Idle Characters	The bit pattern used to signify an idle line. Possible patterns include: • **Flags** • **Mark**
Bandwidth	The effective bandwidth of the PPP session.
Administrative Status	The administrative state of the PPP session: • **Enable** - The PPP session is enabled. • **Disable** - The PPP session is disabled.
VoIP Queue	The state of VoIP queuing on the PPP session. VoIP queuing changes the length of the high priority queue providing support for the configuration of a maximum VoIP delay. Possible states include: • **On** - Voip queuing is active on the PPP session. This enables the device's queues to optimally service VoIP applications. • **Off** - Voip queuing is not active on the PPP session.

Table 7-2. Channel Group Dialog Box - Channel Group Parameters (Continued)

Field	Description
Operational Status	The operational status of the interface. Possible statuses include: • **Up** - The interface is up and can transmit and receive packets. • **Down** - The interface is down due to some failure, and cannot transmit or receive packets. • **Testing** - The interface is in testing mode and cannot transmit or receive regular data. • **Standby** - The interface is a backup interface and cannot transmit or receive packets unless the primary interface it backs up fails. • **Disabled** - The interface is disabled. It cannot transmit or receive packets. • **Partially Down** - The interface is up. However, some interfaces (or PVCs) layered on top of this interface are Down. Some packets can be transmitted and received.

Advanced

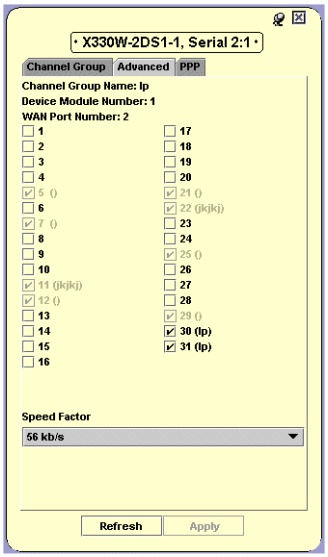
The Advanced tab of the Channel Groups dialog box provides information about the channels that comprise the selected Channel Group and the Channel Group's speed factor.

To view the Advanced tab of the Channel Group dialog box:

1. Click a Channel Group icon in the Chassis View. A list of Channel Groups on the port appears.
2. Click the Channel Group you want to configure. The Channel Group dialog box opens with the Channel Group tab.

3. Click **Advanced**. The Advanced tab of the Channel Group dialog box appears.

Figure 7-4. Channel Group Dialog Box - Advanced Tab



To configure the channels that comprise the Channel Group, check the checkboxes next to the channels you want included in the Channel Group. Uncheck the checkboxes next to the channels you want to remove from the Channel Group.

*** Note:** Channels that belong to other Channel Groups appear gray with the name of the Channel Group to which they belong. These channels cannot be added to the selected Channel Group.

To configure the speed factor of the Channel Group, select a Channel Group speed factor from the Speed Factor pull-down listbox.

PPP

The PPP tab of the Channel Groups dialog box provides configuration information for the PPP interface of the selected Channel Group.

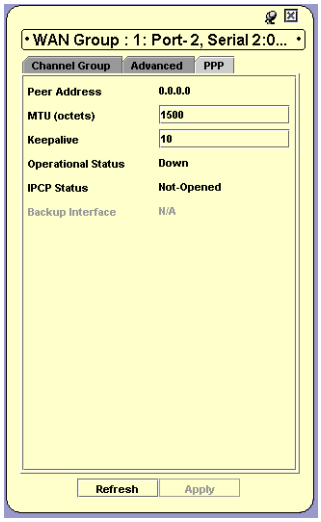
To view the PPP tab of the Channel Group dialog box:

1. Click a Channel Group icon in the Chassis View. A list of Channel Groups on the port appears.

2. Click the Channel Group you want to configure. The Channel Group dialog box opens with the Channel Group tab.

3. Click **PPP**. The PPP tab of the Channel Group dialog box appears.

Figure 7-5. Channel Group Dialog Box - PPP Tab



The following table provides a list of the fields in the PPP tab of the Channel Group dialog box and their descriptions:

Table 7-3. Channel Group Dialog Box - PPP Parameters

Field	Description
Peer Address	The IP address of the PPP session's peer device.
MTU (octets)	The size (in octets) of the largest datagram that can be sent via the PPP session.
Keepalive	The time, in seconds, between keepalive messages. A value of 0 means that keepalive messages are not sent.

Table 7-3. Channel Group Dialog Box - PPP Parameters (Continued)

Field	Description
Operational Status	The operational status of the PPP interface. Possible statuses include: • **Up** - The interface is up and can transmit and receive packets. • **Down** - The interface is down due to some failure, and cannot transmit or receive packets. • **Testing** - The interface is in testing mode and cannot transmit or receive regular data. • **Standby** - The interface is a backup interface and cannot transmit or receive packets unless the primary interface it backs up fails. • **Disabled** - The interface is disabled. It cannot transmit or receive packets. • **Partially Down** - The interface is up. However, some interfaces (or PVCs) layered on top of this interface are Down. Some packets can be transmitted and received.
IPCP Status	IP Control Protocol. The state of IPCP for this PPP session. IP packets can only be transmitted and received over the PPP session when the IPCP status is **Open**. Possible statuses include: • **Open** • **Not-Opened**

Channel Group - Frame Relay Information

The Channel Group dialog box for Channel Groups using frame relay contains five tabs:

- **Channel Group** - Basic information about the Channel Group. For information on the fields in the Channel Group tab of the Channel Group - Frame Relay dialog box, refer to "Channel Group" on page 85.

- **Advanced** - Information about the channels that comprise the Channel Group. For information on the fields in the Advanced tab of the Channel Group - Frame Relay dialog box, refer to "Advanced" on page 87.
- **Frame Relay** - Information about frame relay on the Channel Group.
- **Sub-Interfaces** - Information about the Channel Group's sub-frame relays.
- **DLCIs** - DLCI information for the Channel Group.

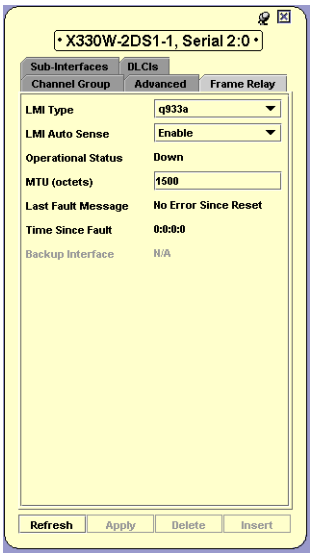
Frame Relay

The Frame Relay tab of the Channel Group dialog box provides information about the frame relay configuration of the Channel Group.

To view the Frame Relay tab of the Channel Group dialog box:

1. Click a Channel Group icon in the Chassis View. A list of Channel Groups on the port appears.
2. Click the Channel Group you want to configure. The Channel Group dialog box opens with the Channel Group tab.
3. Click **Frame Relay**. The Frame Relay tab of the Channel Group dialog box appears.

Figure 7-6. Channel Group Dialog Box - Frame Relay Tab



The following table provides a list of the fields in the Frame Relay tab of the Channel Group dialog box and their descriptions:

Table 7-4. Channel Group Dialog Box - Frame Relay Parameters

Field	Description
LMI Type	Local Management Interface Type. The Data Link Connection Management scheme used by the frame relay interface. Possible values are: • **ANSI** • **q933a** • **lmi-rev1** • **Disable**
LMI AutoSense	Local Management Interface Auto-Sensing is a method for automatically determining the LMI Type for the interface. Possible values are: • **Enable** • **Disable**
Operational Status	The operational status of the interface. Possible statuses include: • **Up** - The interface is up and can transmit and receive packets. • **Down** - The interface is down due to some failure, and cannot transmit or receive packets. • **Testing** - The interface is in testing mode and cannot transmit or receive regular data. • **Standby** - The interface is a backup interface and cannot transmit or receive packets unless the primary interface it backs up fails. • **Disabled** - The interface is disabled. It cannot transmit or receive packets. • **Partially Down** - The interface is up. However, some interfaces (or PVCs) layered on top of this interface are Down. Some packets can be transmitted and received.

Table 7-4. Channel Group Dialog Box - Frame Relay Parameters (Continued)

Field	Description
MTU (octets)	The size (in octets) of the largest datagram that can be sent via the interface.
Last Fault Message	The type of error last occurring on the interface. Possible values are: • **Unknown Error** • **Receive Short** • **Receive Long** • **Illegal Address** • **Unknown Address** • **DLCMI Protocol Error** • **DLCMI Unknown IE** • **DLCMI Sequence Error** • **DLCMI Unknown Rpt** • **No Error Since Reset**
Time Since Fault	The amount of time the system was up before the last error occurred.
Backup Interface	The interface configured to back up the selected interface.

Sub-Interfaces

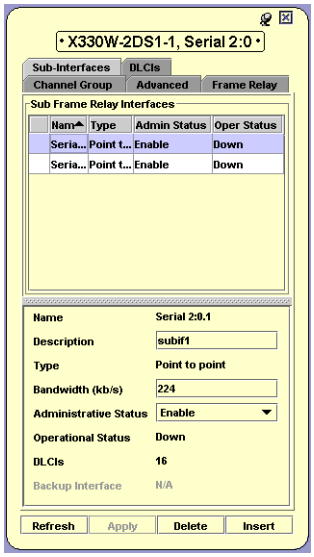
The Sub-Interfaces tab of the Channel Group dialog box provides information about the configuration of Frame Relay sub-interfaces in the Channel Group.

To view the Sub-Interfaces tab of the Channel Group dialog box:

1. Click a Channel Group icon in the Chassis View. A list of Channel Groups on the port appears.
2. Click the Channel Group you want to configure. The Channel Group dialog box opens with the Channel Group tab.

3. Click **Sub-Interfaces**. The Sub-Interfaces tab of the Channel Group dialog box appears.

Figure 7-7. Channel Group Dialog Box - Sub-Interfaces Tab



The Sub-Interfaces tab of the Channel Group dialog box provides a list of Frame Relay sub-interfaces in the upper section of the dialog box. To view configuration information for a specific Frame Relay sub-interface, click the sub-interface in the list. Configuration information for the selected Frame Relay sub-interface appears in the bottom of the dialog box.

You can create, modify, and delete Frame Relay sub-interfaces using the Sub-Interfaces tab of the Channel Group dialog box.

To create a new Frame Relay sub-interface:

1. Click **Insert**. A new row appears in the Sub-Frame-Relay Interfaces list.
2. Enter the parameters for the Frame Relay sub-interface using the fields at the bottom of the dialog box.
3. Click **Apply**. The sub-interface is created.

To modify the parameters of a Frame Relay sub-interface:

1. Click the Frame Relay sub-interface you want to modify. The configuration parameters of the selected sub-interface appear in the bottom of the dialog box.
2. Modify the parameters you want to change using the fields at the bottom of the dialog box.
3. Click **Apply**. The sub-interface parameters are modified.

To delete a Frame Relay sub-interface:

1. Click the Frame Relay sub-interface you want to delete.

*** Note:** You can only delete Frame Relay sub-interfaces on which no IP interfaces are defined.

2. Click **Delete**.

3. Click **Apply**. The sub-interface is deleted.

The following table provides a list of the fields in the Frame Relay Sub-Interfaces tab of the Channel Group dialog box and their descriptions:

Table 7-5. Channel Group Dialog Box - Sub-Interfaces Parameters

Field	Description
Name	The name of the interface.
Description	A user defined description of the sub-interface.
Type	The type of Frame Relay sub-interface. Currently, only Point-to-Point interfaces are supported.
Bandwidth	The bandwidth of the sub-interface in bits per second.
Administrative Status	The administrative status of the interface. Possible statuses include: • **Enable** • **Disable**

Table 7-5. Channel Group Dialog Box - Sub-Interfaces Parameters (Continued)

Field	Description
Operational Status	The operational status of the Frame Relay sub-interface. Possible statuses include: • **Up** - The interface is up and can transmit and receive packets. • **Down** - The interface is down due to some failure, and cannot transmit or receive packets. • **Testing** - The interface is in testing mode and cannot transmit or receive regular data. • **Standby** - The interface is a backup interface and cannot transmit or receive packets unless the primary interface it backs up fails. • **Disabled** - The interface is disabled. It cannot transmit or receive packets. • **Partially Down** - The interface is up. However, some interfaces (or PVCs) layered on top of this interface are Down. Some packets can be transmitted and received.
DLCIs	A list of all DLCIs associated with the Frame Relay sub-interface. If more than one DLCI is configured on the sub-interface, priority DLCI is active. The first DLCI is for high priority traffic, the second DLCI is for medium priority traffic, etc.
Backup Interface	The sub-interface configured to backup this sub-interface.

DLCIs

The DLCIs tab of the Channel Group dialog box provides information about the DLCIs (Data Link Connection Identifiers) in the Channel Group and enables you to create, modify, and delete DLCIs, and associate a DLCI with a specific Frame Relay sub-interface.

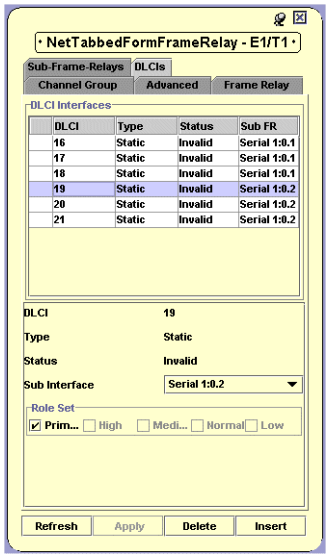
To view the DLCIs tab of the Channel Group dialog box:

1. Click a Channel Group icon in the Chassis View. A list of Channel Groups on the port appears.

2. Click the Channel Group you want to configure. The Channel Group dialog box opens with the Channel Group tab.

3. Click **DLCIs**. The DLCIs tab of the Channel Group dialog box appears.

Figure 7-8. Channel Group Dialog Box - DLCIs Tab



The DLCIs tab of the Channel Group dialog box provides a list of available DLCIs in the upper section of the dialog box. These DLCIs are learned via LMI. To view configuration information for a specific DLCI, click the DLCI in the list. Configuration information for the selected DLCI appears in the bottom of the dialog box.

You can create, modify, and delete DLCIs using the DLCI tab of the Channel Group dialog box.

To create a new DLCI:

1. Click **Insert**. A new row appears in the DLCIs list.

2. Enter the parameters for the DLCI using the fields at the bottom of the dialog box.

3. Click **Apply**. The DLCI is created.

To modify the parameters of a DLCI:

1. Click the DLCI you want to modify. The configuration parameters of the selected DLCI appear in the bottom of the dialog box.

2. Modify the parameters you want to change using the fields at the bottom of the dialog box.

3. Click **Apply**. The DLCI parameters are modified.

To delete a DLCI:

1. Click the DLCI you want to delete.
2. Click **Delete**.
3. Click **Apply**. The DLCI is deleted.

The following table provides a list of the fields in the DLCIs tab of the Channel Group dialog box and their descriptions:

Table 7-6. Channel Group Dialog Box - DLCIs Parameters

Field	Description
DLCI	The DLCI for the circuit.
Type	The method used to create the DLCI. Possible methods include: • **Local** - The DLCI was created manually. • **Unused** - The DLCI was created using the LMI interface.
Status	The operational status of the DLCI. Possible statuses include: • **Active** - The DLCI is active. • **Inactive** - The DLCI is inactive. • **Deleted** - The DLCI has been deleted. • **Invalid** - The DLCI is not valid.
Sub Interface	The Sub-Frame-Relay interface associated with the DLCI.
Role Set	The priority of traffic on the selected DLCI. Possible priorities include: • **Primary** • **High** • **Medium** • **Normal** • **Low**

To configure the priority of DLCI traffic, select the checkboxes for the priorities to use on the DLCI.

If only one DLCI is configured for the Channel Group, all traffic uses the DLCI.

If more than one DLCI is configured on the Channel Group, the priorities must be distributed among the DLCIs, and no priority can be configured on more than one DLCI. For example, if there are three DLCIs configured for a Channel Group, the first DLCI may be configured with **Primary** and **High** priority, the second with **Medium** and **Normal**, and the third with **Low**.

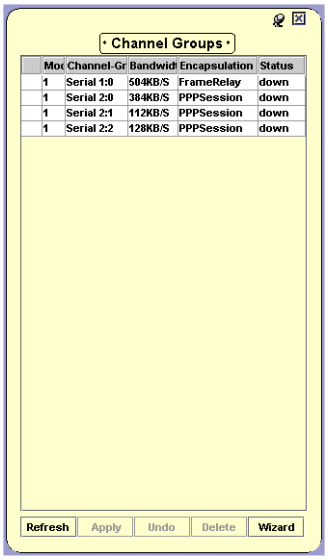
Managing Channel Groups

The Channel Groups dialog box provides information about existing channel groups and enables you to modify and delete channel groups. In addition, you can start the Channel Group Wizard to create and edit channel groups.

Viewing the Channel Groups Table

To view the Channel Groups table, select **Configure > WAN > Channel Groups**. The Channel Groups table opens.

Figure 7-9. Channel Groups Dialog Box



Each row of the Channel Groups table represents a valid Channel Group. The following table provides a list of the fields in the Channel Groups table and their descriptions:

Table 7-7. Channel Groups Table Parameters

Field	Description
Module	The number of the module in which the Channel Group exists.
Channel-Group	The name of the Channel Group.
Bandwidth	The bandwidth of the Channel Group.
Encapsulation	The Channel Group's encapsulation. Possible values are: • **PPP** • **FrameRelay**
Status	The status of the PPP or Frame Relay interface. Possible values are: • **Up** - The interface is up and can transmit and receive packets. • **Down** - The interface is down due to some failure, and cannot transmit or receive packets. • **Testing** - The interface is in testing mode and cannot transmit or receive regular data. • **Standby** - The interface is a backup interface and cannot transmit or receive packets unless the primary interface it backs up fails. • **Disabled** - The interface is disabled. It cannot transmit or receive packets. • **Partially Down** - The interface is up. However, some interfaces (or PVCs) layered on top of this interface are Down. Some packets can be transmitted and received.

Creating, Editing, and Deleting Channel Groups

To create a new channel group, click Wizard in the Channel Groups table. The Channel Group Wizard starts.

To edit a channel group:

1. In the Channel Groups Table, select the channel group which you wish to edit.
2. Click **Wizard**. The Channel Group Wizard starts. The screens in the Channel Group Wizard display the parameters for the selected channel group.

To delete a channel group:

1. In the Channel Groups Table, select the channel group which you wish to delete.
2. Click **Delete**. A confirmation box opens.
3. Click **Yes**. The channel group is deleted.

The Channel Group Wizard

This section provides detailed information on each of the Channel Group Wizard's screens. To continue to the next screen, click **Next**. To return to an earlier screen, click **Back**. To exit the Channel Group Wizard without making any changes, click **Cancel**.

The Channel Group Wizard consists of the following screens:

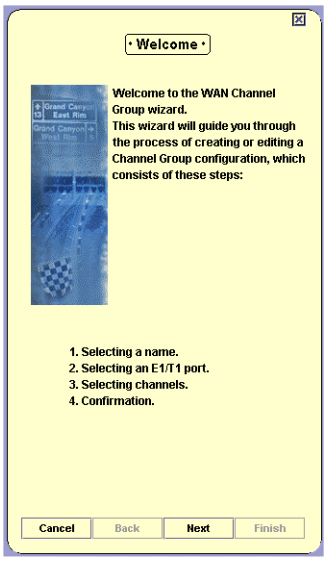
- **Welcome Screen**
- **Select Name and Encapsulation Screen**
- **Select E1/T1 Port Screen**
- **Select Channels and Speed Screen**
- **Confirmation Screen**

The following sections describe each of the Channel Group Wizard screens.

Welcome Screen

The Channel Group Wizard provides a simple, step-by-step method for creating or editing a Channel Group.

Figure 7-10. Channel Group Wizard - Welcome Screen

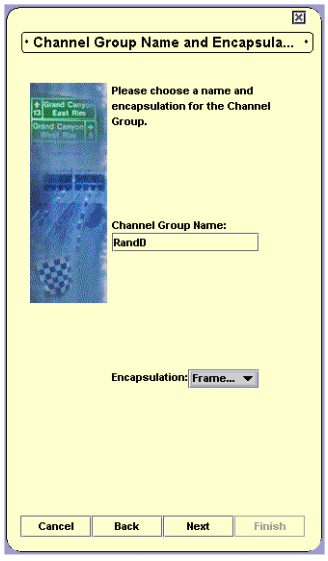

Welcome
Welcome to the WAN Channel Group wizard.
This wizard will guide you through the process of creating or editing a Channel Group configuration, which consists of these steps:
1. Selecting a name.
2. Selecting an E1/T1 port.
3. Selecting channels.
4. Confirmation.
Cancel
Back
Next
Finish

To continue, click **Next**. The Channel Group Wizard continues with the **Select Name and Encapsulation Screen**.

Select Name and Encapsulation Screen

The Select Name and Encapsulation screen enables you to assign a name to the Channel Group and configure the encapsulation method.

Figure 7-11. Channel Group Wizard - Select Name and Encapsulation Screen



Enter a name for the Channel Group in the Channel Group Name field.

Select an encapsulation method for the Channel Group from the pull-down listbox. Available encapsulation methods include:

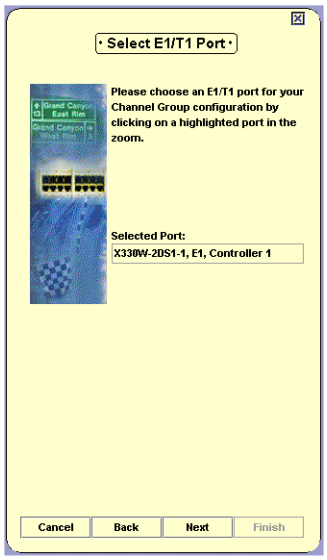
- **PPP** - The Channel Group uses PPP Sessions.
- **FrameRelay** - The Channel Group uses frame relay.

To continue, click **Next**. The Channel Group Wizard continues with the **Select E1/T1 Port Screen**.

Select E1/T1 Port Screen

The Select E1/T1 Port screen enables you to select the E1/T1 port for your channel group.

Figure 7-12. Channel Group Wizard - Select E1/T1 Port Screen

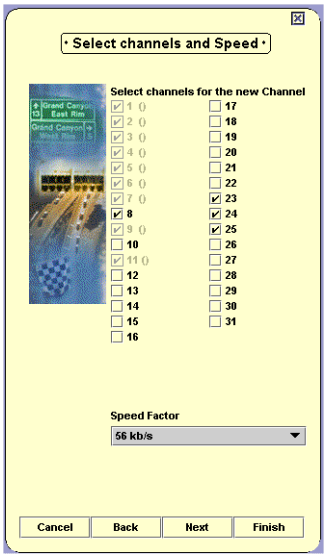

Select E1/T1 Port
Please choose an E1/T1 port for your Channel Group configuration by clicking on a highlighted port in the zoom.
Selected Port:
X330W-2DS1-1, E1, Controller 1
Cancel
Back
Next
Finish

To select an E1/T1 port for the channel group, click an E1/T1 port in the Chassis View. The port designation appears in the Selected Port field. To continue, click **Next**. The Channel Group Wizard continues with the **Select Channels and Speed Screen**.

Select Channels and Speed Screen

The Select Channels and Speed screen enables you to select channels for the new Channel Group.

Figure 7-13. Channel Group Wizard - Select Channels and Speed Screen



To select channels, check the checkboxes next to the channels you want included in the channel group.

For T1 ports, you can also select a speed factor using the Speed Factor pull-down listbox.

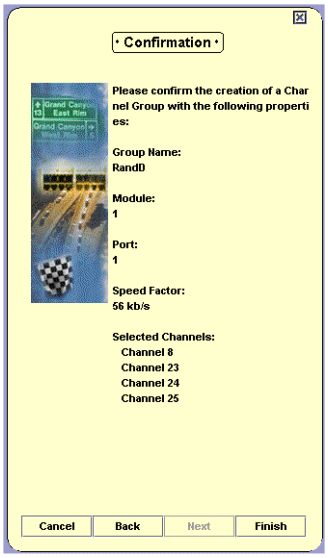
To continue, click **Next**. The Channel Group Wizard continues with the **Confirmation Screen**.

Confirmation Screen

The Channel Group Wizard displays a summary of the information entered using the previous screens.

*** Note:** The Channel Group has not yet been created.

Figure 7-14. Channel Group Wizard - Confirmation Screen



To make any changes to the summary information:

1. Click **Back** until you reach the screen you want.
2. Change the Channel Group's parameters.
3. Click **Next** until you reach the Confirmation screen.

To create the Channel Group or apply the changes to the Channel Group's configuration, click **Finish**. The Channel Group information is uploaded to the device, and the Channel Group table is refreshed.

USP Configuration

The X330WAN expansion module may have USPs (Universal Serial Ports). This section provides information on viewing and configuring USP parameters.

The tabs that appear in the USP dialog box are dependant on the encapsulation method of the selected Channel Group.

To view the USP dialog box, click a USP symbol in the Chassis View or Tree View. The USP dialog box opens to the Serial Port tab.

USP - PPP Interface

For USPs configured with a PPP interface, the USP dialog box contains three tabs:

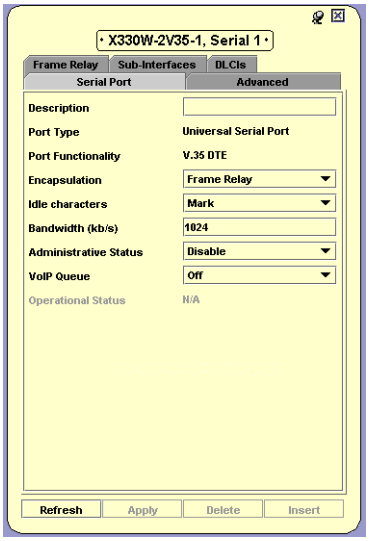
- **Serial Port**
- **Advanced**
- **PPP**

Serial Port

The Serial Port tab of the USP Configuration dialog box provides basic information about the configuration of the USP.

To view the Serial Port tab of the USP Configuration dialog box, click the USP symbol in the Chassis View or the Tree View. The USP Configuration dialog box opens displaying the Serial Port tab.

Figure 7-15. USP Dialog Box - Serial Port Tab



The USP Configuration dialog box provides configuration and status information about the USP.

The following table lists the configuration fields in the Serial Port tab of the USP Configuration dialog box and their descriptions:

Table 7-8. USP Dialog Box - Serial Tab Parameters

Field	Description
Description	The USP port description.
Port Type	The type of port - **Universal Serial Port**.
Port Functionality	The functionality of the port. Possible values include: • **V.35 DTE** • **X.21 DTE** • **EIA530A DTE**
Encapsulation	The encapsulation method for channel groups on the port. Possible methods include: • **PPP** • **Frame Relay**
Idle Characters	The bit pattern used to signify an idle line. Possible patterns include: • **Flags** • **Mark**
Bandwidth	The configured bandwidth of the port in bits per second.
Administrative Status	The state of the selected port. Possible values are: • **Enable** - The port is enabled and can transmit and receive packets. • **Disable** - The port is disabled and cannot transmit or receive packets.
VoIP Queue	The state of VoIP queuing on the PPP session. VoIP queuing changes the length of the high priority queue providing support for the configuration of a maximum VoIP delay. Possible states include: • **On** - Voip queuing is active on the PPP session. This enables the device's queues to optimally service VoIP applications. • **Off** - Voip queuing is not active on the PPP session.

Table 7-8. USP Dialog Box - Serial Tab Parameters (Continued)

Field	Description
Operational Status	The operational status of the interface. Possible statuses include: • **Up** - The interface is up and can transmit and receive packets. • **Down** - The interface is down due to some failure, and cannot transmit or receive packets. • **Testing** - The interface is in testing mode and cannot transmit or receive regular data. • **Standby** - The interface is a backup interface and cannot transmit or receive packets unless the primary interface it backs up fails. • **Disabled** - The interface is disabled. It cannot transmit or receive packets. • **Partially Down** - The interface is up. However, some interfaces (or PVCs) layered on top of this interface are Down. Some packets can be transmitted and received.

Advanced

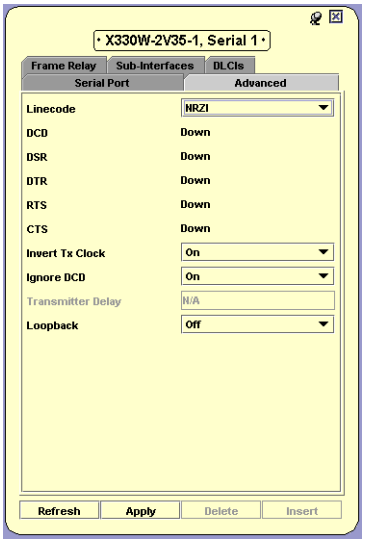
The Advanced tab of the USP Configuration dialog box provides advanced information about the USP configuration.

To display the Advanced tab of the USP Configuration dialog box:

1. Click the USP symbol in the Chassis View or the Tree View. The USP Configuration dialog box opens displaying the Serial Port tab.

2. Click the **Advanced** tab. The Advanced tab of the USP Configuration dialog box appears.

Figure 7-16. USP Configuration Dialog Box - Advanced Tab



The following table lists the configuration fields in the Advanced tab of the USP Configuration dialog box and their descriptions:

Table 7-9. USP Configuration - Advanced Parameters

Field	Description
Clock Source	The clock source for this interface. This value is read-only. Possible values are: • **Internal** • **External** • **Loopback**
Linecode	The type of linecode. Possible values are: • **Nrz** • **Nrzi**
DCD	The port's Data Carrier Detect status. Possible values are: • **Up** - The port has successfully detected Data Carrier. This process takes place during initial line signalling. • **Down** - The port has either not detected Data Carrier or has completed the detection process.

Table 7-9. USP Configuration - Advanced Parameters (Continued)

Field	Description
DSR	The port's Data Set Ready status. Possible values are: • **Up** - The port's data set has successfully been prepared. This process takes place during initial line signalling. • **Down** - The port's data set has either failed preparation or has completed the preparation process.
DTR	The port's Data Terminal Ready status. Possible values are: • **Up** - The port is physically prepared to transmit and receive packets. • **Down** - The port is not physically prepared to transmit and receive packets. This generally indicates an error condition on the circuit.
RTS	The port's Ready To Send status. Possible values are: • **Up** - The port is logically prepared to transmit and receive packets. • **Down** - The port is not logically prepared to transmit and receive packets. This generally indicates an error condition either on the device or the circuit.
CTS	The port's Clear To Send status. Possible values are: • **Up** - The port has successfully completed initial line signalling. CTS takes place at the end of the initial line signalling process and last for a short period of time. • **Down** - The port has either failed to complete initial line signalling or the initial line signalling process has been completed.
Invert Tx Clock	The state of the Tx clock. Possible states are: • **On** - The Tx clock is inverted. • **Off** - The Tx clock is not inverted.

Table 7-9. USP Configuration - Advanced Parameters (Continued)

Field	Description
Ignore DCD	The signal type monitored to determine the interface's status. Possible values are: • **On** - The interface monitors DSR/CTS signals and ignores DCD signals. • **Off** - The interface monitors DCD signals.
transmitter-delay Number	The number of flags transmitted between consecutive frames. Possible values are: • **1** • **2**
Loopback	The status of the DTE loopback. Possible values are: • **On** • **Off**

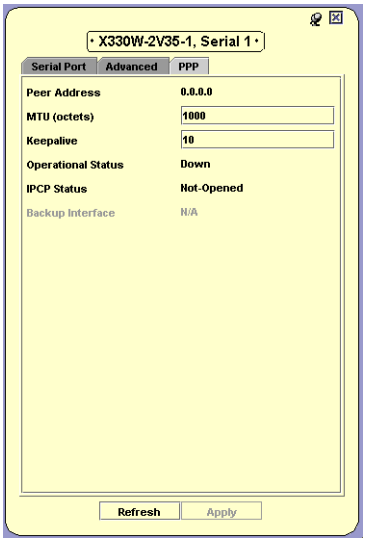
PPP

The PPP tab of the USP Configuration dialog box provides information about the USP's PPP configuration.

To display the PPP tab of the USP Configuration dialog box:

1. Click the USP symbol in the Chassis View or the Tree View. The USP Configuration dialog box opens displaying the Serial Port tab.
2. Click the **PPP** tab. The PPP tab of the USP Configuration dialog box appears.

Figure 7-17. USP Configuration Dialog Box - PPP Tab



The following table lists the configuration fields in the PPP tab of the USP Configuration dialog box and their descriptions:

Table 7-10. USP Configuration - PPP Parameters

Field	Description
Peer Address	The IP address of the PPP session's peer.
MTU	Maximal Transmission Unit. The size of the largest packet that can be transmitted over this PPP session.
Keepalive	The number of seconds between keepalive messages. If this is 0, keepalive messages are not sent.
Operational Status	The operational status of the interface. Possible statuses include: • **Up** - The interface is up and can transmit and receive packets. • **Down** - The interface is down due to some failure, and cannot transmit or receive packets. • **Testing** - The interface is in testing mode and cannot transmit or receive regular data. • **Standby** - The interface is a backup interface and cannot transmit or receive packets unless the primary interface it backs up fails. • **Disabled** - The interface is disabled. It cannot transmit or receive packets. • **Partially Down** - The interface is up. However, some interfaces (or PVCs) layered on top of this interface are Down. Some packets can be transmitted and received.
IPCP Status	IP Control Protocol. The state of IPCP for this PPP session. IP packets can only be transmitted and received over the PPP session when the IPCP status is **Open**. Possible statuses include: • **Open** • **Not-Opened**
Backup Interface	The interface configured to back up this interface.

USP - Frame Relay Interface

For USPs configured with a frame relay interface, the USP dialog box contains five tabs:

- **Serial Port** - Basic information abut the USP. For information on the fields in the Serial Port tab of the USP - Frame Relay dialog box, refer to "Serial Port" on page 106.
- **Advanced** - Information about the channels that comprise the interface. For information on the fields in the Advanced tab of the USP - Frame Relay dialog box, refer to "Advanced" on page 108.
- **Frame Relay** - Information about the frame relay configuration on the USP.
- **Sub-Interfaces** - Information about the Channel Group's Frame Relay sub-interface.
- **DLCIs** - DLCI information for the Channel Group.

Frame Relay

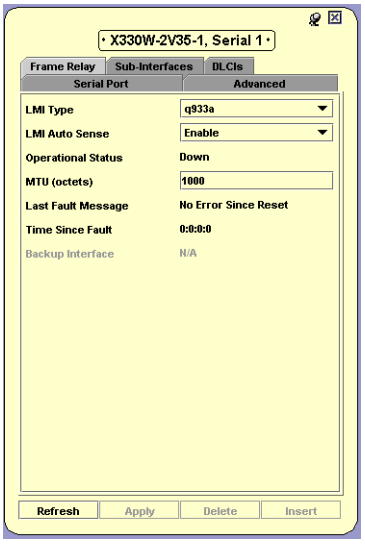
The Frame Relay tab of the USP dialog box provides information about the frame relay configuration of the USP.

To view the Frame Relay tab of the USP dialog box:

1. Click a USP symbol in the Chassis View or Tree View. The USP dialog box opens with the Serial Port tab.

2. Click **Frame Relay**. The Frame Relay tab of the USP dialog box appears.

Figure 7-18. USP Dialog Box - Frame Relay Tab



The following table provides a list of the fields in the Frame Relay tab of the USP dialog box and their descriptions:

Table 7-11. USP Dialog Box - Frame Relay Parameters

Field	Description
LMI Type	Local Management Interface Type. The Data Link Connection Management scheme used by the frame relay interface. Possible values are: • **ANSI** • **q933a** • **lmi-rev1** • **Disable**
LMI Auto Sense	The state of Local Management Interface Auto-Sensing on the interface. Possible states include: • **Enable** - The LMI type is received from the interface at the other end of the line. • **Disable** - The LMI Type is determined by the value in the LMI Type field.

Table 7-11. USP Dialog Box - Frame Relay Parameters (Continued)

Field	Description
Oper Status	The operational status of the interface. Possible statuses include: • **Up** - The interface is up and can transmit and receive packets. • **Down** - The interface is down due to some failure, and cannot transmit or receive packets. • **Testing** - The interface is in testing mode and cannot transmit or receive regular data. • **Standby** - The interface is a backup interface and cannot transmit or receive packets unless the primary interface it backs up fails. • **Disabled** - The interface is disabled. It cannot transmit or receive packets. • **Partially Down** - The interface is up. However, some interfaces (or PVCs) layered on top of this interface are Down. Some packets can be transmitted and received.
MTU (octets)	The size (in octets) of the largest datagram that can be sent via the interface.
Last Fault Message	The type of error last occurring on the interface. Possible values are: • **Unknown Error** • **Receive Short** • **Receive Long** • **Illegal Address** • **Unknown Address** • **DLCMI Protocol Error** • **DLCMI Unknown IE** • **DLCMI Sequence Error** • **DLCMI Unknown Rpt** • **No Error Since Reset**
Time Since Fault	The amount of time the system was up before the last error occurred.

Table 7-11. USP Dialog Box - Frame Relay Parameters (Continued)

Field	Description
Backup INterface	The interface configured to back up this interface.

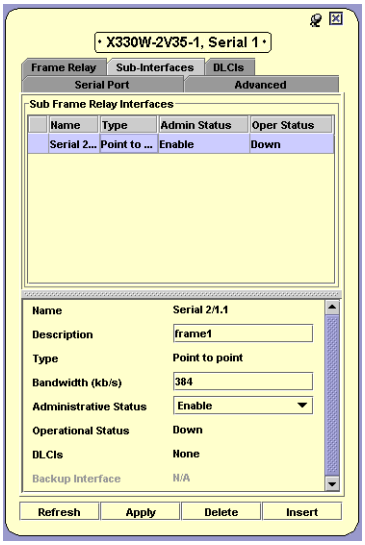
Sub-Interfaces

The Sub-Interfaces tab of the USP dialog box provides information about the configuration of Sub-Frame-Relay interfaces in the USP.

To view the Sub-Interfaces tab of the USP dialog box:

1. Click a USP symbol in the Chassis View or Tree View. The USP dialog box opens with the Serial Port tab.
2. Click **Sub-Interfaces**. The Sub-Interfaces tab of the USP dialog box appears.

Figure 7-19. USP Dialog Box - Sub-Interfaces Tab



The Sub-Interfaces tab of the USP dialog box provides a list of Frame Relay sub-interfaces in the upper section of the dialog box. To view configuration information for a specific Frame Relay sub-interface, click the sub-interface in the list. Configuration information for the selected Frame Relay sub-interface appears in the bottom of the dialog box.

You can create, modify, and delete Frame Relay sub-interfaces using the Sub-Interfaces tab of the USP dialog box.

To create a new Frame Relay sub-interface:

1. Click **New**. A new row appears in the Sub-Frame-Relay Interfaces list.

2. Enter the parameters for the Frame Relay sub-interface using the fields at the bottom of the dialog box.

3. Click **Apply**. The Frame Relay sub-interface is created.

To modify the parameters of a Frame Relay sub-interface:

1. Click the Frame Relay sub-interface you want to modify. The configuration parameters of the selected sub-interface appear in the bottom of the dialog box.

2. Modify the parameters you want to change using the fields at the bottom of the dialog box.

3. Click **Apply**. The Frame Relay sub-interface parameters are modified.

To delete a Frame Relay sub-interface:

1. Click the Frame Relay sub-interface you want to delete.

*** Note:** You can only delete Frame Relay sub-interfaces on which no IP interfaces are defined.

2. Click **Delete**. A confirmation dialog box opens.

3. Click **Yes**.

4. Click **Apply**. The Sub-Frame-Relay interface is deleted.

The following table provides a list of the fields in the Sub-Interfaces tab of the USP dialog box and their descriptions:

Table 7-12. USP Dialog Box - Sub-Interfaces Parameters

Field	Description
Name	The name of the Sub-Frame-Relay interface.
Description	A user defined description of the Sub-Frame-Relay.
Type	The type of Frame Relay sub-interface. Currently, only Point-to-Point interfaces are supported.
Bandwidth	The bandwidth of the Sub-Frame-Relay interface in bits per second.

Table 7-12. USP Dialog Box - Sub-Interfaces Parameters (Continued)

Field	Description
Administrative Status	The state of the selected port. Possible values are: • **Enabled** - The port is enabled and can transmit and receive packets. • **Disabled** - The port is disabled and cannot transmit or receive packets.
Operational Status	The operational status of the Sub-Frame-Relay interface. • **Up** - The interface is up and can transmit and receive packets. • **Down** - The interface is down due to some failure, and cannot transmit or receive packets. • **Testing** - The interface is in testing mode and cannot transmit or receive regular data. • **Standby** - The interface is a backup interface and cannot transmit or receive packets unless the primary interface it backs up fails. • **Disabled** - The interface is disabled. It cannot transmit or receive packets. • **Partially Down** - The interface is up. However, some interfaces (or PVCs) layered on top of this interface are Down. Some packets can be transmitted and received.
DLCIs	A list of all DLCIs associated with the Sub-Frame-Relay interface.
Backup Interface	The interface configured to back up this interface.

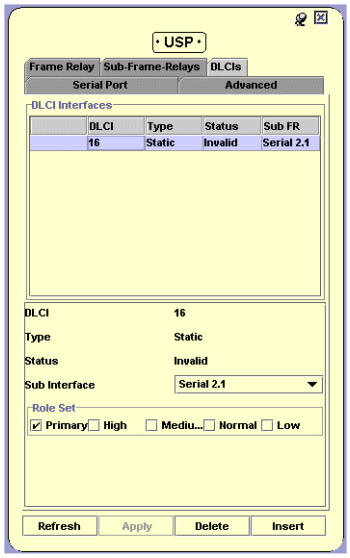
DLCIs

The DLCIs tab of the USP dialog box provides information about the DLCIs in the USP.

To view the DLCIs tab of the USP dialog box:

1. Click a USP symbol in the Chassis View or Tree View. The USP dialog box opens with the Serial Port tab.
2. Click **DLCIs**. The DLCIs tab of the USP dialog box appears.

Figure 7-20. USP Dialog Box - DLCIs Tab



The DLCIs tab of the USP dialog box provides a list of available DLCIs in the upper section of the dialog box. These DLCIs are learned via LMI. To view configuration information for a specific DLCI, click the DLCI in the list. Configuration information for the selected DLCI appears in the bottom of the dialog box.

You can create, modify, and delete DLCIs using the DLCI tab of the USP dialog box.

To create a new DLCI:

1. Click **New**. A new row appears in the DLCIs list.
2. Enter the parameters for the DLCI using the fields at the bottom of the dialog box.
3. Click **Apply**. The DLCI is created.

To modify the parameters of a DLCI:

1. Click the DLCI you want to modify. The configuration parameters of the selected DLCI appear in the bottom of the dialog box.
2. Modify the parameters you want to change using the fields at the bottom of the dialog box.
3. Click **Apply**. The DLCI parameters are modified.

To delete a DLCI:

1. Click the DLCI you want to delete.
2. Click **Delete**. A confirmation dialog box opens.
3. Click **Yes**.
4. Click **Apply**. The DLCI is deleted.

The following table provides a list of the fields in the DLCIs tab of the USP dialog box and their descriptions:

Table 7-13. USP Dialog Box - DLCIs Parameters

Field	Description
DLCI	The DLCI for the circuit.
Type	The method used to create the DLCI. Possible methods include: • **Local** - The DLCI was created manually. • **Unused** - The DLCI was created using the LMI interface.
Status	The operational status of the DLCI. Possible statuses include: • **Active** - The DLCI is active. • **Inactive** - The DLCI is inactive. • **Deleted** - The DLCI has been deleted. • **Invalid** - The DLCI is not valid.
Sub Interface	The Sub-Frame-Relay interface associated with the DLCI.

Table 7-13. USP Dialog Box - DLCIs Parameters (Continued)

Field	Description
Role Set	The priority of traffic on the selected DLCI. Possible priorities include: • **Primary** • **High** • **Medium** • **Normal** • **Low**

To configure the priority of DLCI traffic, select the checkboxes for the priorities to use on the DLCI.

If only one DLCI is configured for the USP, all traffic uses the DLCI.

If more than one DLCI is configured on the USP, the priorities must be distributed among the DLCIs, and no priority can be configured for multiple DLCIs. For example, if there are three DLCIs configured for a USP, the first DLCI may be configured with **Primary** and **High** priority, the second with **Medium** and **Normal**, and the third with **Low**.

Backup Interface Configuration

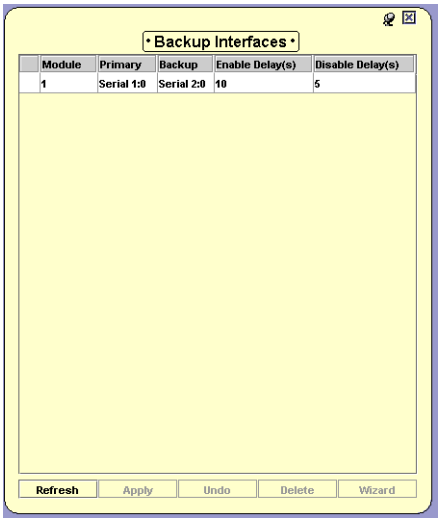
The Backup interface feature enables you to configure Backup interfaces for WAN interfaces. The Backup interface feature includes a table for viewing all configured Backup interfaces and a wizard for creating Backup interfaces.

Viewing the Backup Interfaces Table

The Backup Interfaces table provides a list of all configured Backup interfaces on an X330WAN expansion module.

To view the Backup Interfaces table, select **Configure > WAN > Backup Interfaces**. The Backup Interfaces table opens.

Figure 7-21. Backup Interfaces Table



The Backup Interfaces table provides information about the Backup interfaces configured on the device.

To configure a new Backup interface, click **Wizard**. The Backup Interface Wizard opens. For information on the Backup Interface Wizard, refer to **"The Backup Interface Wizard" on page 124**.

To delete a Backup interface:

1. Select the interface in the table.
2. Click **Delete**. The interface is marked as deleted in the Backup Interfaces table.
3. Click **Apply**. The Backup interface is deleted.

The following table provides a list of fields in the Backup Interfaces table and their descriptions:

Table 7-14. Backup Interfaces Table Parameters

Field	Description
Module	The slot number of the X330WAN expansion module for which the Backup interface is configured.
Primary	The name of the primary interface being backed up.

Table 7-14. Backup Interfaces Table Parameters (Continued)

Field	Description
Backup	The name of the Backup interface.
Enable Delay (s)	The amount of time, in seconds, between the trigger event and the activation of the Backup interface.
Disable Delay (s)	The amount of time, in seconds, between the primary interface returning to an acceptable operational status and the deactivation of the Backup interface.

The Backup Interface Wizard

This section provides detailed information on each of the Backup Interface Wizard's screens. To continue to the next screen, click **Next**. To return to an earlier screen, click **Back**. To exit the Backup Interface Wizard without making any changes, click **Cancel**.

The Backup Interface Wizard consists of the following screens:

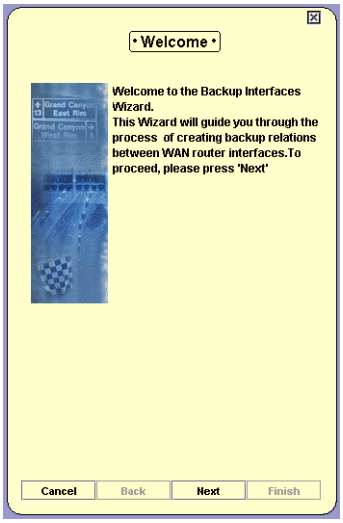
- **Welcome Screen**
- **Select Module Screen**
- **Select Primary Interface Screen**
- **Select Backup Interface Screen**
- **Backup Interface Parameters Screen**
- **Confirmation Screen**

The following sections describe each of the Backup Interface Wizard screens.

Welcome Screen

The Backup Interface Wizard provides a simple, step-by-step method for creating or editing a Backup interface.

Figure 7-22. Backup Interface Wizard - Welcome Screen

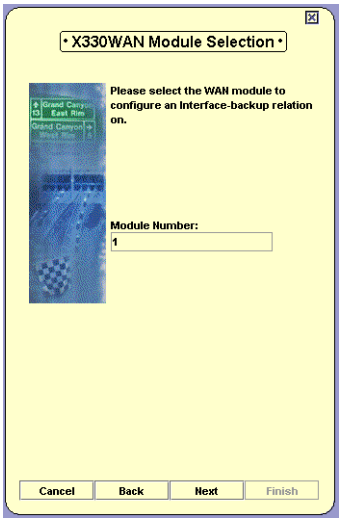

• Welcome •
Welcome to the Backup Interfaces Wizard.
This Wizard will guide you through the process of creating backup relations between WAN router interfaces.To proceed, please press 'Next'
Cancel
Back
Next
Finish

To continue, click **Next**. The Backup Interface Wizard continues with the **Select Module Screen**.

Select Module Screen

The Select Module screen enables you to select the module on which you want to create a Backup interface.

Figure 7-23. Backup Interface Wizard - Select Module Screen



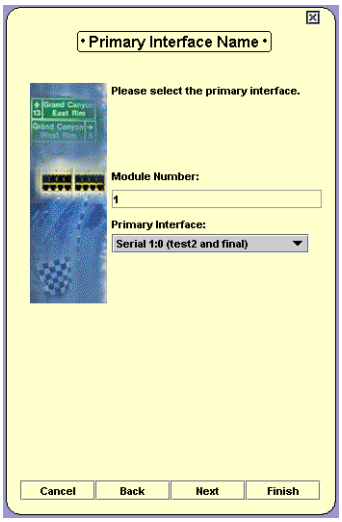
Select an X330WAN module from the Chassis View or Tree View. The module number appears in the Module Number field.

To continue, click **Next**. The Backup Interface Wizard continues with the **Select Primary Interface Screen**.

Select Primary Interface Screen

The Select Primary Interface screen enables you to select the interface to be backed up.

Figure 7-24. Backup Interface Wizard - Select Primary Interface Screen



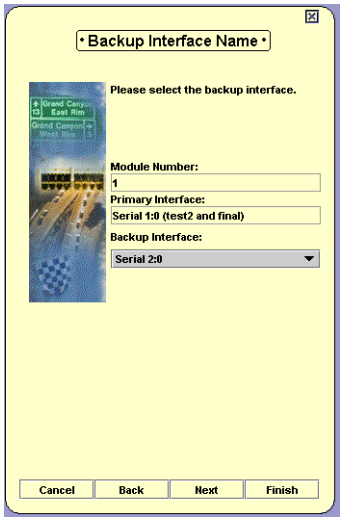
To select an interface to back up, select an interface name from the Primary Interface pull-down listbox.

To continue, click **Next**. The Backup Interface Wizard continues with the **Select Backup Interface Screen**.

Select Backup Interface Screen

The Select Backup Interface screen enables you to assign an interface to back up the primary interface.

Figure 7-25. Backup Interface Wizard - Select Backup Interface Screen



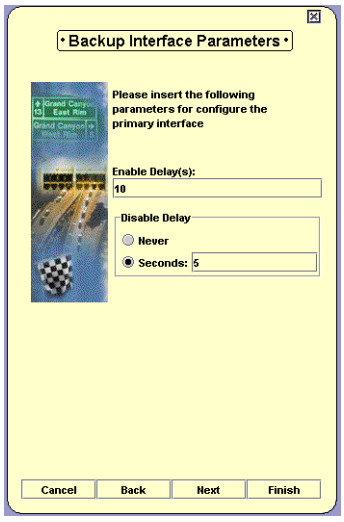
To select a Backup interface, select an interface name from the Backup Interface pull-down listbox.

To continue, click **Next**. The Backup Interface Wizard continues with the **Backup Interface Parameters Screen**.

Backup Interface Parameters Screen

The Backup Interface Parameters screen enables you to configure the conditions under which the Backup interface is activated and deactivated.

Figure 7-26. Backup Interface Wizard - Backup Interface Parameters Screen



To configure the number of seconds between the failure of the primary interface and the activation of the Backup interface, enter a number in the Enable Delay field.

To configure the action taken when the primary interface returns to an acceptable operational status:

- To prevent the deactivation of the Backup interface, click **Never**. The Backup interface remains activated.
- To configure the number of seconds between the primary interface returning to an acceptable operational status and the deactivation of the Backup interface:

  a. Click **Seconds:**.

  b. Enter the number of seconds to wait in the available field.

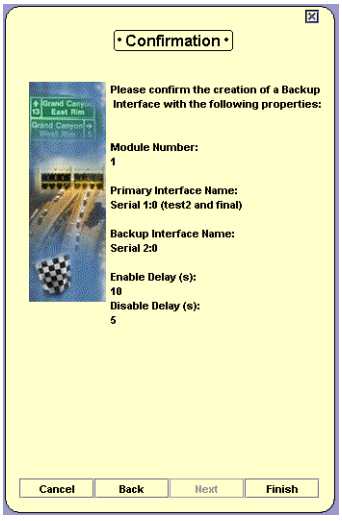
To continue, click **Next**. The Backup Interface Wizard continues with the **Confirmation Screen**.

Confirmation Screen

The Backup Interface Wizard displays a summary of the information entered using the previous screens.

*** Note:** The Backup Interface has not yet been created.

Figure 7-27. Backup Interface Wizard - Confirmation Screen



To make any changes to the summary information:

1. Click **Back** until you reach the screen you want.
2. Change the Backup interface's parameters.

3. Click **Next** until you reach the Confirmation screen.

To create the Backup interface or apply the changes to the Backup interface's configuration, click **Finish**. The Backup interface information is uploaded to the device, and the Backup Interfaces table is refreshed.

8 Port RMON

This chapter explains the port RMON options of the Avaya C360 Device.

To view Port RMON information, you must be in Port RMON mode. To switch to Port RMON mode:

Click .

Or

Select **View > Port RMON**.

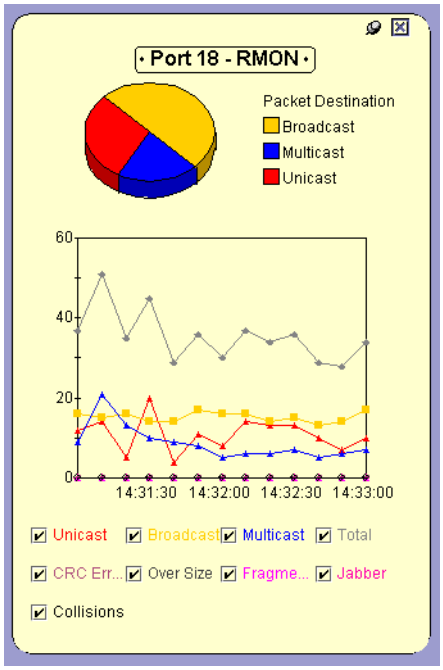
For more information on RMON, refer to *RMON* in *The Reference Guide*.

*** Note:** Port RMON is not available when running the Avaya C360 Manager via Web Management.

Displaying the Port RMON Window

To display the Port RMON window, select a port or a LAG in the Chassis or Tree View. The Port RMON window opens.

Figure 8-1. Port RMON Window



The Port RMON window includes three sections. At the top of the window is a pie chart. In the center of the window is a graph. At the bottom of the window is a list of traffic types.

The Pie Chart

The pie chart shows the relative amounts of Unicast and Non-Unicast traffic on a selected port or LAG. The legend to the right of the pie chart shows the color representing each of the traffic types.

The Traffic Graph

The graph charts various traffic types over time. Each traffic type is represented by a different colored line. Using the mouse, you can view traffic statistics, zoom in or out of the graph, and scroll within the graph to view parts of the graph that are currently hidden.

When changing the view on the graph, the graph freezes. To unfreeze the graph and restore the display to the default display, click on the graph.

Viewing Traffic Statistics

To view traffic statistics, hold the mouse over a point on the graph representing the traffic for which you would like to see statistics. After two seconds, an info box appears displaying the name of the traffic type represented by the line in the graphic, and the traffic rate at the selected point.

Zooming In and Out of the Graph

To zoom out and view a graph of all the traffic on the selected port from the time the application was opened, double-click the graph. The graph is compressed to show all of the traffic on the port from the time the application was opened until now.

To zoom in on a portion of the graph, press **SHIFT** and select a portion of the graph using the mouse. The graph zooms in and shows only the portion of the graph that was selected.

Scrolling within the Graph

To scroll within the graph, hold the left mouse button down while moving the mouse from the graph in the direction you want to scroll. The graph scrolls in the selected direction.

Unfreezing the Graph

When zooming or scrolling within the graph, the display freezes and is not updated with the current information. To reactivate the display, click anywhere in the graph. The graph display is restored to normal, and the graph is reactivated.

Traffic Types

The bottom of the Port RMON window contains a list of various types of traffic. Each traffic type has a checkbox next to it. Only traffic types whose checkboxes are checked are displayed in the Port RMON graph.

The following table provides a list of the traffic types and their descriptions.

Table 8-1. Traffic Types

Field	Description
Collisions	Total number of Ethernet collisions in which the port was involved.
CRC Errors	Total number of Ethernet packets received at this port with FCS error and Framing error. This indicates the number of corrupted packets received.

Table 8-1. Traffic Types (Continued)

Field	Description
Fragments	Total number of Ethernet packets received at this port whose octet count is less than the minimum standard packet length.
Frames Too Long	Total number of Ethernet packets received at this port whose octet count is more than the maximum standard packet length.
Jabber	Total number of Ethernet packets received at this port that are too long and include CRC errors.
Non-Unicast	Total number of good packets directed to non-unicast addresses that were received on the port.
Total Packets Received	Total number of packets of valid frame length that were received on the port.
Unicast	Total number of good packets received that were directed to a unicast address.

9 VLANs

This chapter provides the information and instructions you need to use VLANs. It includes the following topics:

- **VLAN Configuration Overview** - An overview of VLANs and their components.
- **Viewing the VLAN Configuration Dialog Box** - Instructions on how to access the VLAN Configuration dialog box and a description of the VLAN Configuration dialog box.
- **Managing VLANs** - Instructions on how to create, delete, and rename VLANs.
- **Viewing Port VLAN Settings** - Instructions on how to view VLAN settings for ports on the device.
- **Managing Port VLAN Settings** - Instructions on how to configure VLAN settings for ports on the device.
- **Updating the Device** - Instructions on how to update the device with new VLAN information.

*** Note:** In this chapter, ports include LAGs. i.e. Any mention of a port refers to a port or LAG.

VLAN Configuration Overview

This section contains an overview of VLANs and how to configure them, and contains the following sections:

- **VLANs Overview**
- **Master VLAN List**
- **VLAN Tags**

VLANs Overview

The building blocks of VLANs are switch ports. To build a new VLAN you need to define a VLAN name and number. You can then add switch ports to the VLAN by configuring the PVID of the port to the VLAN number. The ports are members of the VLAN whose number is their PVID. In addition, you can configure the VLAN tagging mode and binding style of the switch ports. VLAN #1 is the default VLAN and is named **Default**.

For more information about VLANs, refer to *VLANs* in *The Reference Guide.*

Master VLAN List

The master VLAN list is a file on the network management station that contains a list of globally defined VLANs and their names. This list is only available when running Avaya MultiService Network Manager. It is not available when running an Embedded Web Manager. To manage the master VLAN list, use Avaya VLAN Manager. For information on Avaya VLAN Manager, refer to the *Avaya MultiService VLAN Manager User Guide*.

VLANs that are listed in the master VLAN list are called globally known VLANs. VLANs that are not in the master VLAN list but are configured on a device are called locally known VLANs.

VLAN Tags

Packets can be tagged with VLAN information. When a tagged packet enters a switch port, it maintains its tag. When an untagged packet enters a switch port, the packet is tagged with the port's PVID (Port VLAN ID).

When a packet arrives at the egress port, the VLAN Binding Style is checked. If the packet's VLAN tag does not match a VLAN to which the egress port is bound, the packet is discarded. If the tag matches a VLAN to which the egress port is bound, the Tagging Mode is used. If the Tagging Mode is Clear, the packet is forwarded with no VLAN tag. If the Tagging Mode is anything else, the packet is forwarded with its VLAN tag.

Viewing the VLAN Configuration Dialog Box

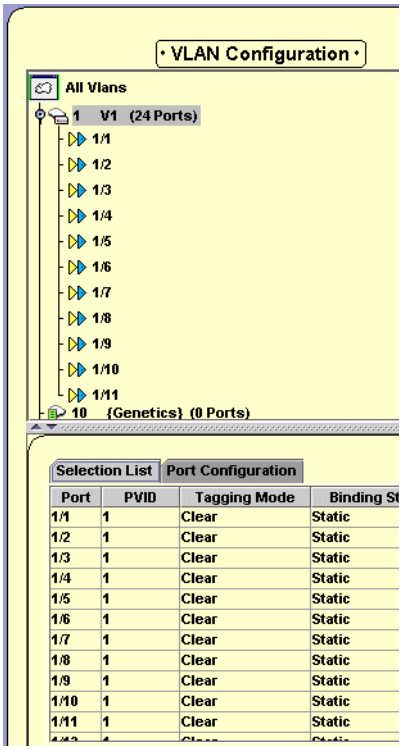
To view VLAN names, numbers, and component switch ports:

Click .

Or

Select **Configure > VLANs**. The VLAN Configuration dialog box opens.

Figure 9-1. VLAN Configuration Dialog Box



The VLAN Configuration dialog box consists of the following components:

- **VLAN Tree**
- **Selection List**
- **Port Configuration Area**

To refresh the information in the VLAN Configuration dialog box and lose all unapplied changes, click **Refresh**.

To resize the three areas of the VLAN Configuration dialog box, use the splitter bars.

VLAN Tree

A tree providing a list of VLANs and their ports. The VLANs include all VLANs known on the network and all VLANs configured on the device. The ports listed under a VLAN include member ports and ports statically bound to the VLAN.

To expand or contract a branch of the table:

Double-click the VLAN's name.

Or

Click the handle next to the VLAN's name.

The VLAN symbol includes a green tag if the VLAN is listed in the master VLAN list, and a device symbol if it exists locally on the device. If it is listed in the master VLAN list and exists locally on the device, the VLAN symbol includes a green tag and a device symbol.

If the VLAN name on the device differs from the globally defined VLAN name, the local VLAN name appears after the VLAN number, followed by the global VLAN name in braces. For example, if VLAN 4 is locally named **RandD**, and globally named **Research**, the following string will appear in the VLAN Tree: **`4 RandD {Research}`**. To change all locally defined VLAN names to the globally defined names, you can synchronize the VLAN names on the device. For information on synchronizing VLAN names, refer to "Synchronizing VLAN Names" on page 144.

*** Note:** When using the Embedded Web Device Manager, global VLAN information is not available.

The VLAN's member ports appear with a yellow triangle and blue triangle next to the port name. Ports that are statically bound to the VLAN appear with a blue triangle attached to the port name. Member ports are automatically bound to the VLANs of which they are members. Ports whose VLAN information has changed but has not been applied, appear with gray triangles.

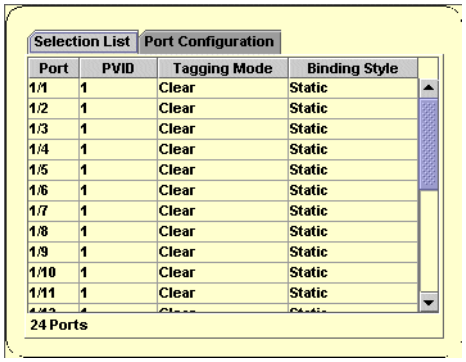
When a VLAN is selected in the VLAN Tree, member ports appear in the Chassis View with a yellow triangle and blue triangle on the port symbol, and statically bound ports appear in the Chassis View with a blue triangle on the port symbol. In addition, information about the member ports and statically bound ports appear in the Selection List.

For more information about the Selection List, refer to "Selection List" on page 139.

Selection List

The Selection List contains a table with VLAN information about the current selection. For example, if you select a module in the Tree View or Chassis View, a list of the ports in the module with their VLAN information appears in the Selection List. If the Port Configuration Area is open, click **Selection List**. The Selection List appears.

Figure 9-2. Selection List



The following table provides a list of the information fields in the Selection List and their descriptions.

Table 9-1. Selection List Fields

Field	Description
Port	The module and port number.
PVID	The Port VLAN ID (PVID) of the port. This is the VLAN of which the port is a member.
Tagging Mode	The tagging mode of the port. For information on tagging modes, refer to "Port Configuration Area" on page 140.
Binding Style	The binding style configured on the port. For information on binding styles, refer to "Port Configuration Area" on page 140.

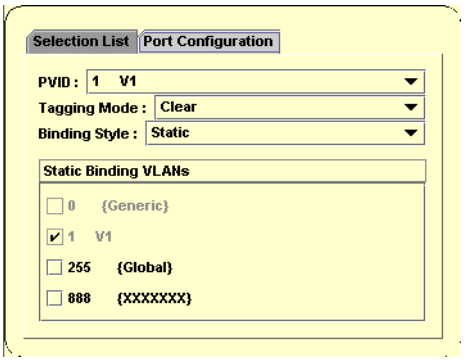
To sort the Selection List table by any of its fields, click the field header. To reverse the order of the sort, click the field header a second time.

The information in the Selection List is read-only.

Port Configuration Area

The Port Configuration Area enables you to configure a port's VLAN configuration. To view the Port Configuration Area, click **Port Configuration**. The Port Configuration Area appears.

Figure 9-3. Port Configuration Area



The following table provides a list of the configuration parameters in the Port Configuration Area and their description.

Table 9-2. Port Configuration Area Parameters

Field	Description
PVID	The Port VLAN ID (PVID) of the port. This is the VLAN of which the port is a member. The PVID pull-down list contains all VLANs known to the network and VLANs on the device.
Tagging Mode	The tagging mode of the port. The tagging mode controls the tagging of packets that can be forwarded by the port. The following tagging modes are available: • **Clear** - The packet is forwarded with no VLAN tag. • **IEEE-802.1Q** - The packet is forwarded with a VLAN tag in conformance with the IEEE-802.q standard.

Table 9-2. Port Configuration Area Parameters (Continued)

Field	Description
Binding Style	The binding style configured on the port. The binding style defines which packets can be forwarded by the port. The following binding styles are available: • **Bind to All** - The port is bound to all VLANs known to the device. This is also known as persistent binding. If a packet is on a VLAN not known to the device, the packet is discarded. • **Bind to Configured** - The port is bound to all VLANs known to the device and to the VLANs with which packets reaching the ports are tagged. This is also known as dynamic binding. If a packet is on a VLAN not known to the device, the packet is discarded. • **Static** - The port is bound to the VLANs checked in the Static Binding VLANs list. Packets on all other VLANs are discarded.
Static Binding VLANs	A list of VLANs known on the network and VLANs configured on the device. Each VLAN has an accompanying checkbox. Possible values are: • **Checked** - The VLAN is bound to the port being configured. • **Unchecked** - The VLAN is not bound to the port being configured. *** Note:** The settings are only used when the port is configured with the **Static** Binding Style.

Managing VLANs

You can create, delete, and rename VLANs.

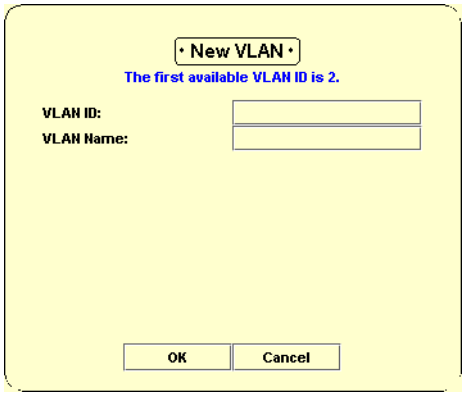
- **Creating VLANs**
- **Deleting VLANs**
- **Renaming VLANs**

Creating VLANs

To create a new VLAN:

1. Click **New**. The Create VLAN dialog box opens.

Figure 9-4. Create VLAN Dialog Box



2. Enter a VLAN number in the VLAN ID field.

*** Note:** The range of valid VLAN numbers is 1 to 3071.

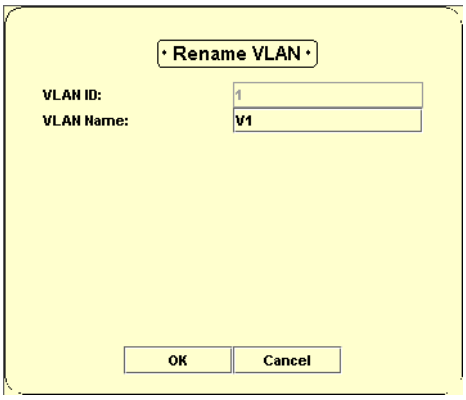
3. Enter a name for the VLAN in the VLAN Name field.
4. Click **OK**. The new VLAN is created.

Renaming VLANs

To rename a VLAN:

1. Select the VLAN whose name you want to edit.
2. Click **Rename**. The Rename VLAN dialog box opens.

Figure 9-5. Rename VLAN Dialog Box



3. Edit the VLAN's name in the VLAN Name field.
4. Click **OK**. The VLAN is renamed.

Synchronizing VLAN Names

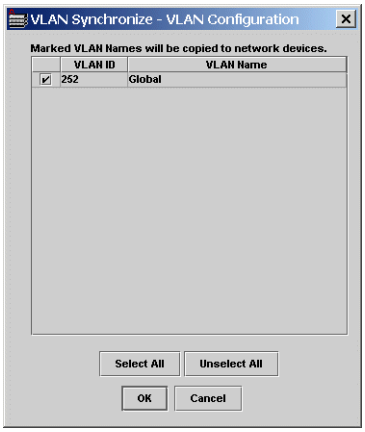
VLANs with the same VLAN number can be defined with different names on different devices in the network. In addition, VLAN names can be configured in the master VLAN list. This can cause confusion when referring to a VLAN by name rather than by number. The VLAN application enables you to synchronize the VLAN names on the device with those in the master VLAN list.

When synchronizing the VLAN names on the device with those in the master VLAN list, the VLANs on the device are renamed to provide consistency with the names in the master VLAN list.

To synchronize VLAN names on the device with the master VLAN list:

1. Click **Sync**. The VLAN Synchronize dialog box opens. The VLAN Synchronize dialog box contains a list of VLANs whose local names differ from the VLAN names in the master VLAN list. The following fields appear for each VLAN:
   - **VLAN ID** - The VLAN number (ID) for the VLAN.
   - **VLAN Name** - The VLAN name in the master VLAN list.

Figure 9-6. VLAN Synchronize Dialog Box



2. Check the checkboxes next to the VLANs whose names you want to synchronize.
   - To select all the VLANs in the VLAN Synchronize dialog box, click **Select All**.
   - To unselect all the VLANs in the VLAN Synchronize dialog box, click **Unselect All**.

3. Click **OK**. The marked VLANs on the device are renamed with the VLAN names in the master VLAN list.

Deleting VLANs

You can delete VLANs from the Avaya C360 Device. Globally known VLANs can be deleted from the device, but not from the master VLAN list. If you delete a VLAN that is on the master VLAN list and on the device, the VLAN remains in the VLAN Tree with a green tag.

To delete a VLAN:

1. Select the VLAN you want to delete.
2. Ensure that there are no member ports associated with the VLAN.
3. Click **Delete**. The VLAN is deleted from the device.

Managing Port VLAN Settings

You can view and configure the PVID, Tagging Mode, and Binding Style of selected ports using the Selection List and Port Configuration Area. In addition, you can configure the PVID of selected ports using the drag-and-drop method.

Selecting Ports

This section explains how to select ports for VLAN configuration.

Ports can be selected from the Tree View, Chassis View, or VLAN Tree for VLAN Configuration.

- To select a port, click the port in the Tree View, Chassis View, or VLAN Tree.
- To select multiple ports, press **CTRL** while selecting additional ports.
- To select all of the ports on a module, click the module icon in the Tree View or Chassis View.
- To select all of the ports on the device, click the device icon in the Tree View or Chassis View.

- To select all of the ports associated with a VLAN (including member ports and statically bound ports), click the VLAN in the VLAN Tree.

Viewing Port VLAN Settings

To view the VLAN configuration of a port, select a port in the Tree View, Chassis View, or VLAN Tree. The port's VLAN configuration appears in the Selection List. If you select multiple ports in the Tree View, Chassis View, or VLAN Tree, the VLAN configurations for all of the selected ports appear in the Selection List. In addition, parameters that are common to all ports in the selection appear in the Port Configuration Area.

For details on the information provided in the Selection List, refer to "Selection List" on page 139.

Using the Port Configuration Area

To configure the VLAN setting for ports on the device using the Port Configuration Area:

1. Click **Port Configuration**. The Port Configuration Area appears.
2. Select the ports you want to configure in the Tree View, Chassis View, or VLAN Tree. The settings that are common to all of the selected ports appear in the fields in the Port Configuration Area. For information on selecting ports, refer to "Selecting Ports" on page 145.
3. Change the settings in the Port Configuration Area using the pull-down lists and checkboxes. For information on the settings in the Port Configuration Area, refer to "Port Configuration Area" on page 140. The VLAN configuration for the selected ports is changed.

*** Note:** When changing the PVID of the selected ports, the ports do not appear selected in the VLAN Tree. However, the ports remain in the Selection List.

Drag-and-Drop

To configure the PVID of ports using drag-and-drop:

1. Select the ports you want to configure in the Tree View, Chassis View, or VLAN Tree. For information on selecting ports, refer to "Selecting Ports" on page 145.

2. Drag the ports until they are over a VLAN icon in the VLAN Tree. The ports are added to the desired VLAN.

*** Note:** When dragging ports from the VLAN Tree, only ports represented by PVID symbols are added to the desired VLAN. Dragged static binding icons are ignored and do not change port PVIDs.

Updating the Device

Ports whose VLAN information has changed appear dimmed in the VLANs table. To update the device with the changes, click **Apply**.

For more information on the user interface, refer to "Using Dialog Boxes and Tables" on page 16.

10 Link Aggregation Groups

This chapter provides the information and instructions for creating and using Link Aggregation Groups (LAGs). It includes the following topics:

- **LAGs Overview** - An overview of LAGs.
- **Viewing the LAG Table** - Instructions on accessing the LAG Table and a description of the LAG Table.
- **Creating LAGs** - Instructions on creating LAGs.
- **Editing LAGs** - Instructions on editing LAGs.
- **The LAG Wizard** - Detailed descriptions of the screens in the LAG Wizard.
- **Deleting LAGs** - Instructions on deleting LAGs.

For information on configuring LAGs, refer to "Viewing LAG Configuration" on page 31.

LAGs Overview

Link Aggregation Groups (LAGs) provide a method of creating a high-bandwidth link. A LAG consists of a group of ports acting as a single logical port. All ports participating must have the same configuration.

For more information on LAGs, refer to *Link Aggregation Groups (LAGs)* in *The Reference Guide*.

Viewing the LAG Table

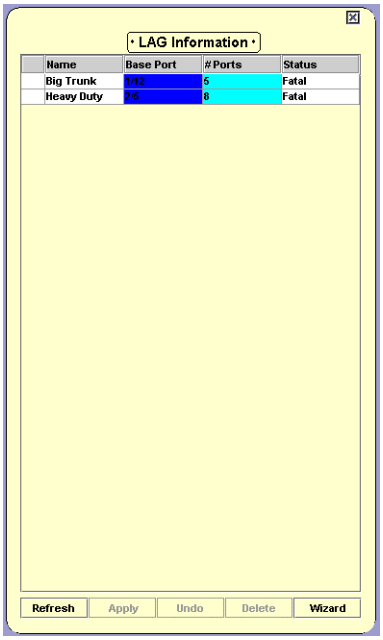
To view the LAG Table:

Click .

Or

Select **Configure > LAG**. The LAG Information table opens.

Figure 10-1. LAG Information Dialog Box



Each row of the LAG table represents a valid Link Aggregation Group and provides the following information:

- **Name** - The LAG name.
- **Base Port** - The number of the LAG's base port.
- **# of Ports** - The number of ports assigned to the LAG.
- **Status** - The warning status of the LAG.

When a LAG is selected, the ports in the LAG appear highlighted in the Chassis and Tree View.

Creating LAGs

To create a new LAG, click **Wizard**. The LAG Wizard starts.

For more information, refer to "The LAG Wizard" on page 151.

Editing LAGs

To edit an existing LAG:

1. Select a LAG by clicking on the row representing the LAG.
2. Click **Wizard**. The LAG Wizard starts.

When editing a LAG, the LAG Wizard's dialog boxes display the current LAG configuration parameters. To keep the values currently displayed in one of the dialog boxes, click **Next**. If you have changed some of the LAG's parameters, and you want to keep the rest of the LAG's configuration, click **Finish**. The device is updated with the LAG's new configuration.

For more information, refer to "The LAG Wizard" on page 151.

The LAG Wizard

This section provides detailed information on each of the LAG Wizard's screens. To continue to the next screen, click **Next**. To return to an earlier screen, click **Back**. To exit the LAG Wizard without making any changes, click **Cancel**.

The LAG Wizard consists of the following screens:

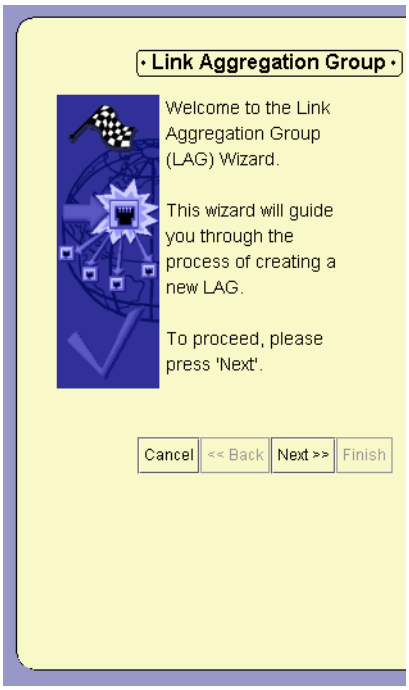
- **Welcome Screen**
- **Base Port Selection Screen**
- **Member Port Selection Screen**
- **LAG Name Screen**
- **Confirmation Screen**

The following sections describe each of the LAG Wizard screens.

Welcome Screen

The LAG Wizard provides a simple, step-by-step method for creating a LAG.

Figure 10-2. LAG Wizard - Welcome Screen


Link Aggregation Group
Welcome to the Link Aggregation Group (LAG) Wizard.
This wizard will guide you through the process of creating a new LAG.
To proceed, please press 'Next'.
Cancel
<< Back
Next >>
Finish

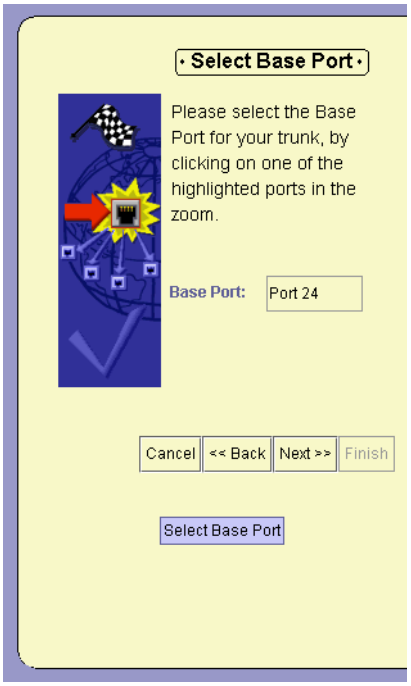
To continue, click **Next**. The LAG Wizard continues with the **Base Port Selection Screen**.

Base Port Selection Screen

The Base Port Selection screen of the LAG Wizard helps you select a base port for the LAG. The attributes of the base port (port speed, port mode, etc.) are applied to the other member ports of the LAG. Ports which can be selected as base ports appear white in the Chassis View.

*** Note:** Ports that participate in a Port Redundancy cannot be assigned to a LAG.

Figure 10-3. LAG Wizard - Base Port Selection Screen


· Select Base Port ·
Please select the Base Port for your trunk, by clicking on one of the highlighted ports in the zoom.
Base Port:
Port 24
Cancel
<< Back
Next >>
Finish
Select Base Port

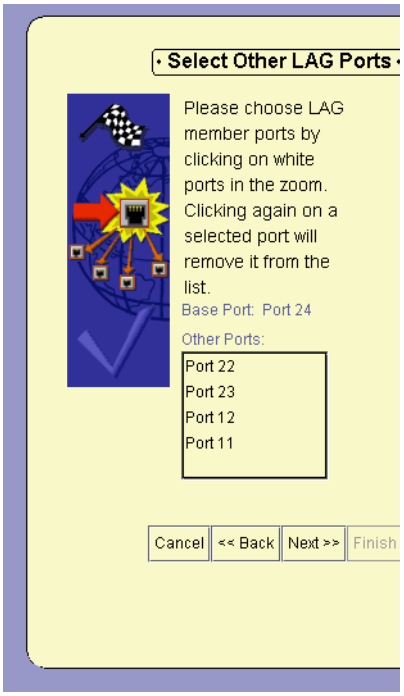
To select a base port for the LAG, click a port in the Chassis View. The selected port is listed in the Base Port field of the wizard and appears blue in the Chassis View and Tree View.

When you have selected the base port for the LAG, click **Next**. The LAG Wizard continues with the **Member Port Selection Screen**.

Member Port Selection Screen

The Member Port Selection screen of the LAG Wizard helps you select additional ports for the LAG. Ports which can be selected as additional ports appear in white in the Chassis View.

Figure 10-4. LAG Wizard - Member Port Selection Screen


Select Other LAG Ports
Please choose LAG member ports by clicking on white ports in the zoom. Clicking again on a selected port will remove it from the list.
Base Port: Port 24
Other Ports:
Port 22
Port 23
Port 12
Port 11
Cancel
<< Back
Next >>
Finish

To select additional ports for the LAG, click ports in the Chassis View. The selected ports appear cyan in the Chassis View and Tree View and are listed in the Other Ports field in the wizard.

To remove selected ports from the list, click the selected ports in the Chassis View. The selected ports appear white in the Chassis View and Tree View and are removed from the Other Ports field in the wizard.

When you have finished selecting the additional ports for the LAG, click **Next**. The LAG Wizard continues with the **LAG Name Screen**.

LAG Name Screen

The LAG Name screen of the LAG Wizard enables you to assign a name to the LAG.

Figure 10-5. LAG Wizard - LAG Name Screen

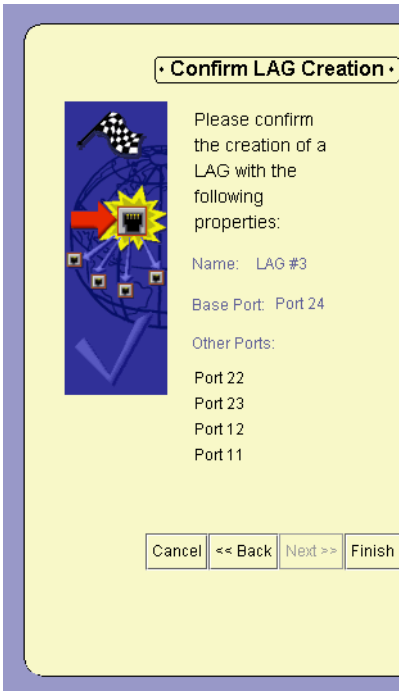
To assign a name to the LAG, enter the name for the LAG in the LAG Name field.

When you have entered a name for the LAG, click **Next**. The LAG Wizard continues with the **Confirmation Screen**.

Confirmation Screen

The LAG Wizard displays a summary of the LAG information entered using the previous screens. The LAG has not yet been created.

Figure 10-6. LAG Wizard - Confirmation Screen



To make any changes to the summary information:

1. Click **Back** until you reach the screen you want.
2. Change the LAG's parameters.
3. Click **Next** until you reach the Confirmation screen.

To create the LAG or apply the changes to the LAG's configuration, click **Finish**. The LAG information is uploaded to the device, and the LAG table is refreshed.

Deleting LAGs

To delete an existing LAG:

1. Click the row representing the LAG you want to delete.
2. Click **Delete**.
3. The LAG is marked with the symbol.
4. Click **Apply** to update the device.

For more information on the user interface, refer to "Using Dialog Boxes and Tables" on page 16.

For more information on tables, refer to "Managing Tables" on page 5.

11 Port Redundancy

This chapter provides the information and instructions for using the Port Redundancy feature. It includes the following topics:

- **Overview of Port Redundancy** - An overview of port redundancy.
- **Viewing the Port Redundancy Dialog Box** - Instructions on accessing the Port Redundancy dialog box, and a description of the Port Redundancy dialog box.
- **Adding a Port Redundancy** - Instructions on configuring a new port redundancy.
- **Port Redundancy Wizard** - Detailed descriptions of the screens in the Port Redundancy Wizard.
- **Deleting Port Redundancies** - Instructions on deleting port redundancies.
- **Updating the Device** - Instructions on updating the device with the changes made to the Port Redundancy dialog box.

Overview of Port Redundancy

Port Redundancy enables you to define a redundancy relationship between any two ports or LAGs in a device, or between a port and a LAG. One port or LAG is defined as the primary port and the other as the secondary port. In case the primary port link fails, the secondary port takes over. This connection between the two ports is called a Port Redundancy.

An Intermodule Port Redundancy provides a port redundancy service that operates even when the primary port link fails as the result of a failure of the module. For example, if the module on which the primary port in an Intermodule Port Redundancy is located powers down or is removed from the device, the secondary port in the Intermodule Port Redundancy takes over.

*** Note:** Only one intermodule port redundancy can be configured on a device.

Individual member ports of a LAG can not participate in a Port Redundancy. However, you can define Port Redundancy on a complete LAG.

*** Note:** To edit Port Redundancy information, you must delete the Port Redundancy, and create a new one.

For more information on Port Redundancy, refer to *Redundancy* in *The Reference Guide*.

Viewing the Port Redundancy Dialog Box

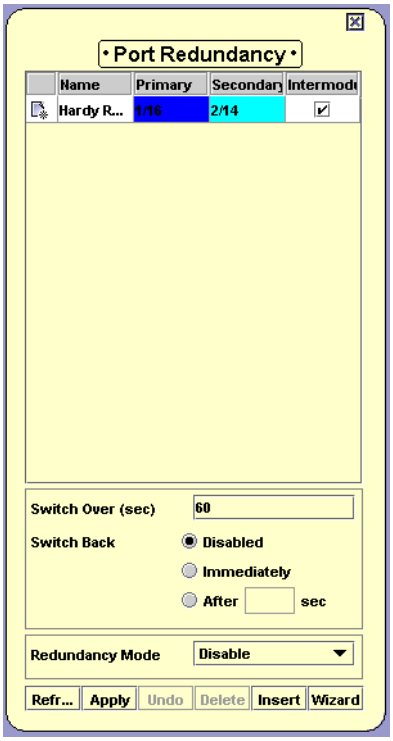
To view the Port Redundancy dialog box:

Click .

Or

Select **Configure > Port Redundancy**. The Port Redundancy dialog box opens.

Figure 11-1. Port Redundancy Dialog Box



The Port Redundancy dialog box provides a list of all port redundancies configured on the switch, with their respective primary and secondary ports and the device's port redundancy configuration.

The following table provides a list of the fields in the Port Redundancy dialog box and their descriptions:

Table 11-1. Port Redundancy Fields - 802.1x Tab

Field	Description
Name	The name of the port redundancy.
Primary	The primary port of the port redundancy pair.
Secondary	The secondary port of the port redundancy pair.
Intermodule	If checked, the port redundancy is an intermodule port redundancy. If not checked, the port redundancy is not an intermodule port redundancy.
Switch Over (sec)	The minimum time between switching between the ports in a port redundancy pair.
Switch Back	The amount of time after the primary port link is reestablished after which the primary port takes over from the secondary port. Possible values include: • **Disabled** - The primary port does not take over from the secondary port. • **Immediately** - The primary port takes over from the secondary port as soon as the primary port link is reestablished. • **After** *x* **sec**- The primary port takes over from the secondary port *x* seconds after the primary port link is reestablished.
Redundancy Mode	State of Port Redundancy on the Avaya C360 device. Possible values are: • **Enabled** - Port Redundancy is enabled on this device. • **Disabled** - Port Redundancy is not enabled on this device.

To configure the device's port redundancy configuration:

1. Enter an amount in the Switch Over field.
2. Select one of the Switch Back option buttons.
3. If you selected **After** *x* **sec**, enter the number of seconds for the switch back in the **After** *x* **sec** field.

4. Update the device. For more information on updating the device, refer to "Updating the Device" on page 169.

Adding a Port Redundancy

To add a new Port Redundancy:

1. Click **Wizard**. The Port Redundancy Wizard starts. For more information, refer to "Port Redundancy Wizard" on page 163.

Or

1. Click **Insert**. A row is added to the Port Redundancy dialog box.
2. Enter a name for the Port Redundancy in the Name field.
3. Select a port or a LAG from the Tree View or the Chassis View and drag it to the Primary Port field. The port number or LAG name appears in the Primary Port field.
4. Select a port or a LAG from the Tree View or the Chassis View and drag it to the Secondary Port field. The port number or LAG name appears in the Secondary Port field.
5. To configure the port redundancy as an extra resilient port redundancy, check the **Intermodule** checkbox.

*** Note:** Only one intermodule port redundancy can be configured on a device.

6. Update the device. For more information on updating the device, refer to "Updating the Device" on page 169.

*** Note:** A port cannot participate in more than one redundancy scheme.

Port Redundancy Wizard

This section provides detailed information on each of the Port Redundancy Wizard's screens. To continue to the next screen, click **Next**. To return to an earlier screen, click **Back**. To exit the Port Redundancy Wizard without making any changes, click **Cancel**.

The Port Redundancy Wizard consists of the following screens:

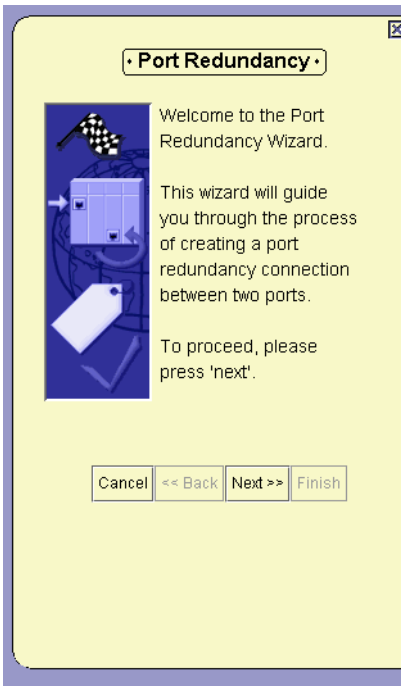
- **Welcome Screen**
- **Primary Port Selection Screen**
- **Secondary Port Selection Screen**
- **Name and Type Screen**
- **Confirmation Screen**

The following sections describe each of the Port Redundancy Wizard screens.

Welcome Screen

The Port Redundancy Wizard provides a simple, step-by-step method for creating a Port Redundancy.

Figure 11-2. Port Redundancy Wizard - Welcome Screen

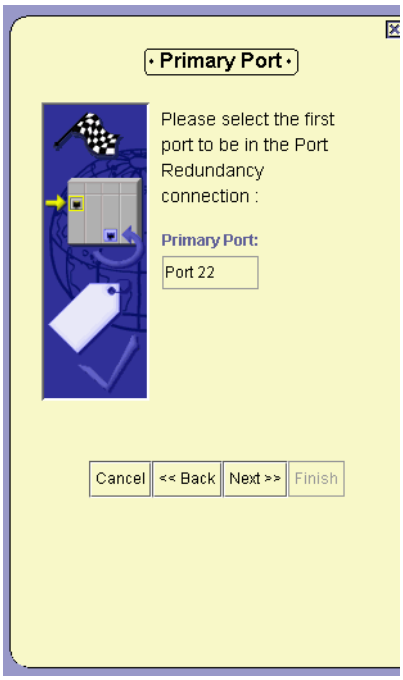

Port Redundancy
Welcome to the Port Redundancy Wizard.
This wizard will guide you through the process of creating a port redundancy connection between two ports.
To proceed, please press 'next'.
Cancel
<< Back
Next >>
Finish

To continue, click **Next**. The Port Redundancy Wizard continues with the **Primary Port Selection Screen**.

Primary Port Selection Screen

The Primary Port Selection screen of the Port Redundancy Wizard helps you select a primary port for the Port Redundancy. Ports and LAGs which can be selected as primary ports appear in white in the Chassis View.

Figure 11-3. Port Redundancy Wizard - Primary Port Selection Screen



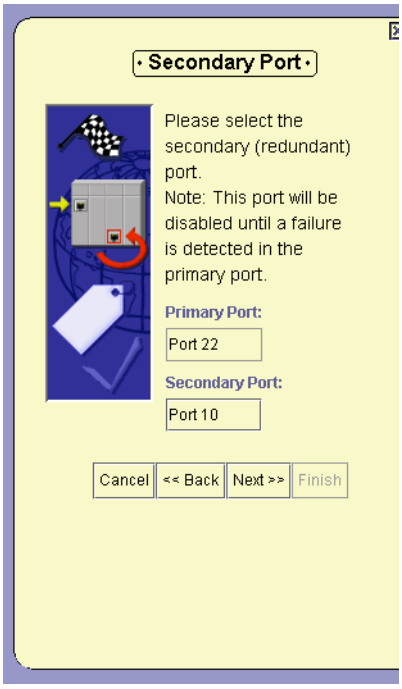
To select a primary port for the Port Redundancy, click a port or LAG in the Chassis View. The selected port or LAG appears blue in the Chassis View and Tree View and is listed in the Primary Port field in the wizard.

When you have selected the primary port for the Port Redundancy, click **Next**. The Port Redundancy Wizard continues with the **Secondary Port Selection Screen**.

Secondary Port Selection Screen

The Secondary Port Selection screen of the Port Redundancy Wizard allows you to select a secondary port for the Port Redundancy. Ports and LAGs that can be selected as secondary ports appear white in the Chassis View.

Figure 11-4. Port Redundancy Wizard - Secondary Port Selection Screen



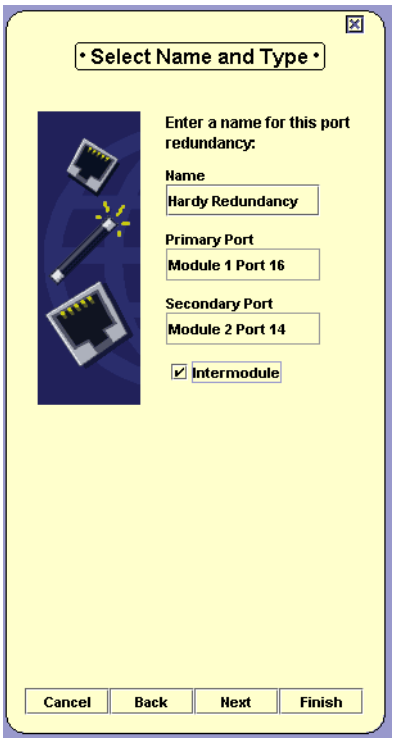
To select a secondary port for the Port Redundancy, click a port or LAG in the Chassis View. The selected port or LAG appears cyan in the Chassis View and Tree View, and is listed in the Secondary Port field in the wizard.

When you have finished selecting the secondary port for the Port Redundancy, click **Next**. The Port Redundancy Wizard continues with the **Name and Type Screen**.

Name and Type Screen

The Port Redundancy Name and Type screen of the Port Redundancy Wizard allows you to assign a name for the Port Redundancy, and determine if the redundancy is an intermodule port redundancy.

Figure 11-5. Port Redundancy Wizard - Name and Type Screen



To assign a name to the Port Redundancy, enter the name for the Port Redundancy in the Name field.

To configure the redundancy as an intermodule Port Redundancy, check the Intermodule checkbox.

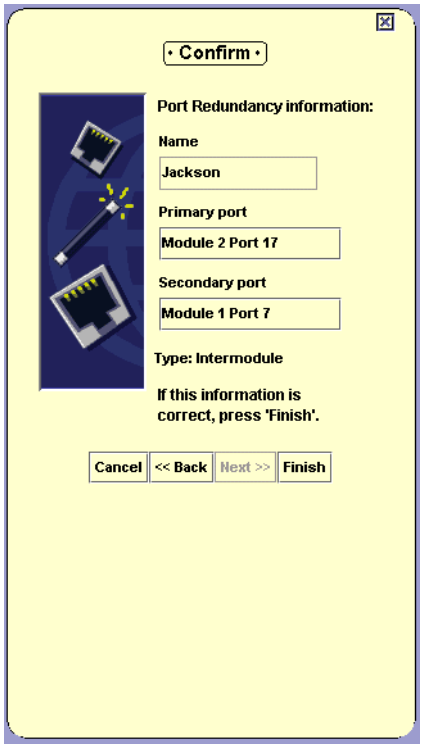
*** Note:** If an intermodule port Redundancy is already configured on the device, the Intermodule checkbox does not appear.

When you have selected a name and a type for the Port Redundancy, click **Next**. The Port Redundancy Wizard continues with the **Confirmation Screen**.

Confirmation Screen

The Port Redundancy Wizard displays a summary of the Port Redundancy information entered using the previous screens. The Port Redundancy has not yet been created.

Figure 11-6. Port Redundancy Wizard - Confirmation Screen



To make any changes to the summary information:

1. Click **Back** until you reach the screen you want.
2. Change the Port Redundancy's parameters.
3. Click **Next** until you reach the Confirmation screen.

To create the Port Redundancy, click **Finish**. The Port Redundancy information is uploaded to the device, and the Port Redundancy dialog box is refreshed.

Deleting Port Redundancies

To delete an existing Port Redundancy:

1. Select a Port Redundancy from the Port Redundancy dialog box.
   - To select more than one Port Redundancy, press **CTRL** while clicking on additional Port Redundancies.
2. Click **Delete**. The selected Port Redundancies are marked with the symbol.

Updating the Device

To update the device with all changes made to the Port Redundancy dialog box, click **Apply**. The device is updated with all new information.

To discard all changes made to the Port Redundancy dialog box, click **Refresh**. All changes made to the Port Redundancy dialog box are discarded.

For more information on the user interface, refer to "Using Dialog Boxes and Tables" on page 16.

For more information on tables, refer to "Managing Tables" on page 5.

12 Port Mirroring

This chapter provides the information and instructions for using the Port Mirroring feature. It includes the following topics:

- **Port Mirroring Overview** - An overview of port mirroring.
- **Configuring Port Mirroring** - Instructions on adding, editing, and deleting a port mirroring pair.
- **The Port Mirroring Wizard** - Detailed descriptions of the screens in the Port Mirroring Wizard.

Port Mirroring Overview

Port Mirroring copies all received and transmitted packets (including local traffic) from a source port to a predefined destination port, in addition to the normal destination port of the packets. This is a useful method for monitoring all traffic traveling through a specific port.

For more information on Port Mirroring, refer to *Port Mirroring* in *The Reference Guide*.

CAUTION

Do not change the VLAN of the source or destination port while the port mirroring mechanism is operating.

Configuring Port Mirroring

This section explains how to configure Port Mirroring on the Avaya C360 Device.

To configure Port Mirroring:

Click .

Or

Select **Configure > Port Mirroring**. The Port Mirroring Wizard opens.

The Port Mirroring Wizard

This section provides detailed information on each of the Port Mirroring Wizard's screens. To continue to the next screen, click **Next**. To return to an earlier screen, click **Back**. To exit the Port Mirroring Wizard without making any changes, click **Cancel**.

The Port Mirroring Wizard consists of the following screens:

- **Create Welcome Screen**
- **Edit/Delete Welcome Screen**
- **Source Port Selection Screen**
- **Destination Port Selection Screen**
- **Frames Direction Selection Screen**
- **Confirmation Screen**

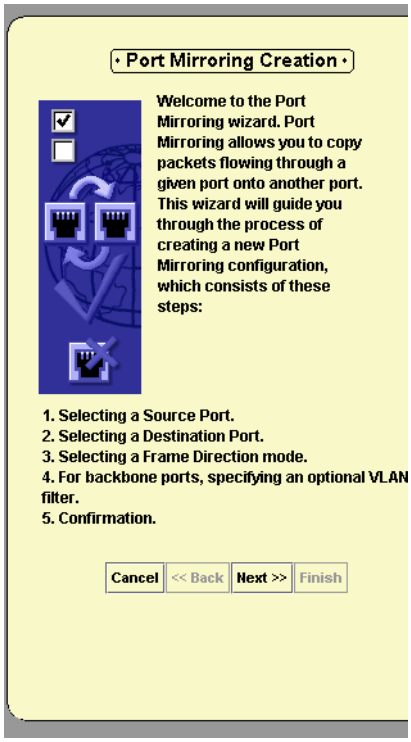
If Port Mirroring is not currently active on the device, the Port Mirroring Wizard starts with the Create Welcome screen. If Port Mirroring is currently active on the device, the Port Mirroring Wizard starts with the Edit/Delete Welcome screen.

The following sections describe each of the Port Mirroring Wizard screens.

Create Welcome Screen

The Port Mirroring Wizard provides a simple, step-by-step method for defining a Port Mirroring pair.

Figure 12-1. Port Mirroring Wizard - Create Welcome

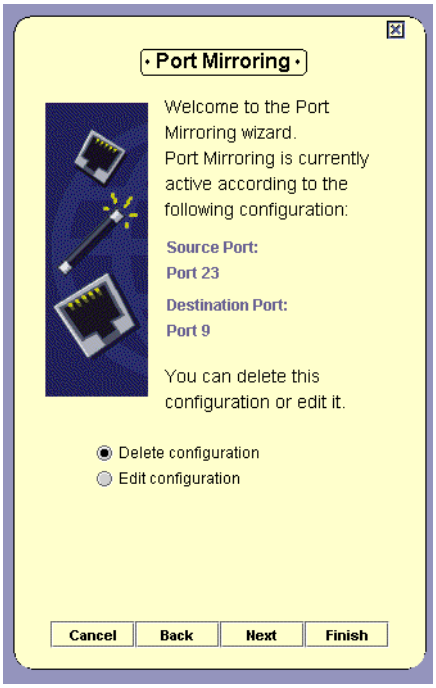

Port Mirroring Creation
Welcome to the Port Mirroring wizard. Port Mirroring allows you to copy packets flowing through a given port onto another port. This wizard will guide you through the process of creating a new Port Mirroring configuration, which consists of these steps:
1. Selecting a Source Port.
2. Selecting a Destination Port.
3. Selecting a Frame Direction mode.
4. For backbone ports, specifying an optional VLAN filter.
5. Confirmation.
Cancel
<< Back
Next >>
Finish

To continue, click **Next**. The Port Mirroring Wizard continues with the **Edit/Delete Welcome Screen**.

Edit/Delete Welcome Screen

The wizard offers the choice of deleting or editing the existing Port Mirroring configuration.

Figure 12-2. Port Mirroring Wizard - Edit/Delete Welcome Screen



To delete the existing Port Mirroring configuration:

1. Select the **Delete configuration** option button.
2. Click **Next**. The Port Mirroring Wizard continues with the **Confirmation Screen** screen.

To edit the existing Port Monitoring configuration:

1. Select the **Edit configuration** option button.
2. Click **Next**. The Port Mirroring Wizard continues with the **Source Port Selection Screen**. The current configuration is reflected in the wizard's screens.

Source Port Selection Screen

The Source Port Selection screen of the Port Mirroring Wizard helps you select a source port for the Port Mirroring pair. Ports which can be selected as sources appear in white in the Chassis View.

Figure 12-3. Port Mirroring Wizard - Source Port Selection Screen

Select Source Port
Please select the Source Port for your Port Mirroring configuration by clicking on one of the highlighted ports in the zoom.
Source Port:
Port 9 Module 1
Cancel
<< Back
Next >>
Finish

To select a source for the Port Mirroring pair, select a highlighted port in the Chassis View. The selected port appears blue in the Chassis View and Tree View and is listed in the Source Port field in the wizard.

When you have selected the source for the Port Mirroring, click **Next**. The Port Mirroring Wizard continues with the **Destination Port Selection Screen**.

Destination Port Selection Screen

The Destination Port Selection screen of the Port Mirroring Wizard helps you select a destination port or LAG for the Port Mirroring pair. Ports and LAGs which can be selected as destinations appear white in the Chassis View.

Figure 12-4. Port Mirroring Wizard - Destination Port Selection Screen

Select Destination Port
Please choose the Destination Port for your Port Mirroring configuration by clicking on a highlighted port in the zoom.
Source Port:
Port 9 Module 1
Destination Port:
Port 22 Module 1
Cancel
<< Back
Next >>
Finish

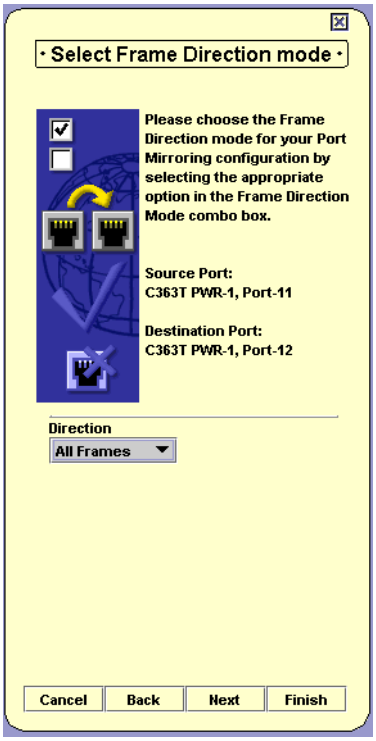
To select a destination for the Port Mirroring pair, select a port or LAG in the Chassis View. The selected port or LAG appears cyan in the Chassis View and Tree View and is listed in the Destination Port field in the wizard.

When you have finished selecting the destination for the Port Mirroring pair, click **Next**. The Port Mirroring Wizard continues with the **Frames Direction Selection Screen**.

Frames Direction Selection Screen

The Frames Direction Selection screen of the Port Mirroring Wizard enables you to select the traffic to be copied to the destination port. You can configure the destination port to receive all traffic going through the source port, or only the traffic received by the source port.

Figure 12-5. Port Mirroring Wizard - Frames Direction Selection Screen



To configure which frames are copied to the destination port, select an option from the Direction pull-down list box. Possible options are:

- **All Frames** - All traffic going through the source port is copied to the destination port.
- **Rx Frames** - Traffic received by the source port is copied to the destination port.
- **Tx Frames** - Traffic transmitted by the source port is copied to the destination port.

When you have finished selecting the traffic to be copied, click **Next**. The Port Mirroring Wizard continues with the **Confirmation Screen**.

Confirmation Screen

The Port Mirroring Wizard displays a summary of the Port Mirroring information entered using the previous screens. The Port Mirroring configuration has not yet been uploaded to the device.

Figure 12-6. Port Mirroring Wizard - Confirmation Screen

To make any changes to the summary information:

1. Click **Back** until you reach the screen you want.
2. Change the Port Mirroring parameters.
3. Click **Next** until you reach the Confirmation screen.

To upload the Port Mirroring configuration to the device, click **Finish**. The Port Mirroring configuration is uploaded to the device.

13 IP Multicast Filtering

This chapter provides information on configuring IP Multicast Filtering on the Avaya C360 Device. It includes the following sections:

- **IP Multicast Filtering Overview** - A brief overview of IP Multicast Filtering.
- **Configuring IP Multicast Filtering** - Instructions on accessing the IP Multicast Filtering dialog box and descriptions of the parameters in the IP Multicast Filtering dialog box.

IP Multicast Filtering Overview

IP Multicast Filtering provides a method for distributing high-bandwidth applications to specific stations that may be configured on different VLANs. It allows for a single copy of the data to be propagated on the network, copied only when the paths to endstations diverge.

Configuring IP Multicast Filtering

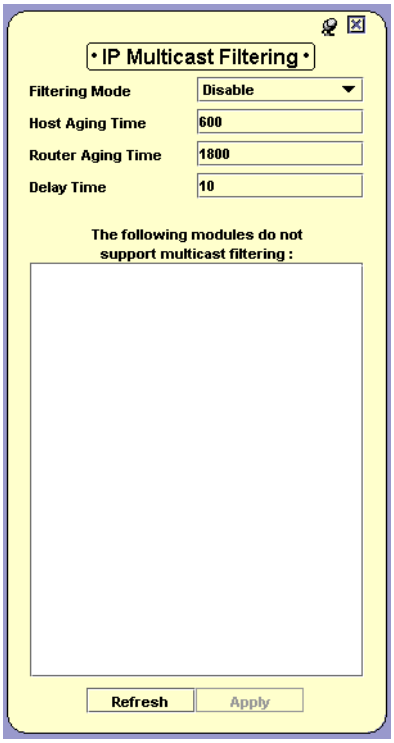
To configure IP Multicast Filtering:

Click .

Or

Select **Configure > IP Multicast Filtering**. The IP Multicast Filtering dialog box opens.

Figure 13-1. IP Multicast Filtering Dialog Box



The IP Multicast Filtering dialog box enables you to configure IP Multicast filtering parameters on the Avaya C360 Device.

The following table provides a list of the fields in the IP Multicast Filtering dialog box and their descriptions:

Table 13-1. IP Multicast Filtering Parameters

Field	Description
Filtering Mode	The mode of operation of the IP Multicast Filtering on the device. Possible Modes are: • **Enable** - IP Multicast Filtering is enabled on the device. • **Disable** - IP Multicast Filtering in not enabled on the device.
Host Aging Time	The amount of time (in seconds) allowed to pass from a router's last IP Multicast request before the device stops forwarding all multicast sessions to a router. The valid range for this parameter is 30 - 7200 seconds.
Router Aging Time	The amount of time (in seconds) allowed to pass from a remote router's last IP Multicast request before the local router's multicast routing table stops forwarding all multicast sessions to the remote router. The valid range for this parameter is 30 - 7200 seconds.
Delay Time	The amount of time (in seconds) the device waits from receiving a request for a new IP Multicast session until IP Multicast filtering begins. This time allows other hosts to report to the device. The valid range for this parameter is 1 - 300 seconds.

To change the IP Multicast filtering configuration for the Avaya C360 Device, change the IP Multicast filtering parameters.

To apply the changes, click **Apply**.

To refresh the information in the IP Multicast Filtering dialog box, click **Refresh**.

14 Trap Managers Configuration

This chapter provides the information and instructions for configuring managers for the Avaya C360 Device. It includes the following topics:

- **Trap Manager Overview** - An overview of trap managers.
- **Viewing the Stack Trap Managers Table** - Instructions on accessing the device's Trap Managers Table, and a description of the Trap Managers Table.
- **Viewing the Media Gateway Trap Managers Table** - Instructions on accessing the Media Gateway Trap Managers Table, and a description of the Media Gateway TrapMedia Gateway Table.
- **Viewing the WAN Trap Managers Table** - Instructions on accessing the WAN Trap Managers Table, and a description of the WAN Trap Managers Table.
- **Editing the Trap Managers Table**- Instructions on how to edit the Trap Managers Table.

Trap Manager Overview

In the event of a fault or an unusual occurrence, the Avaya C360 can send traps to one or more Network Management Stations (NMS). To enable this feature, you must configure the Avaya C360 with a list of the managers' workstations. Traps are then sent to the stations listed in the Managers table.

*** Note:** Up to ten managers can be assigned per device. However, it is recommended to keep the list limited to actual and relevant managers so as not to place undue stress on the network.

Using the Trap Managers Table, you can also configure which traps are sent to specific managers. The columns to the right of the managers' IP addresses represent specific traps. Checking the checkbox in a trap column enables the manager to receive the checked trap. Managers only receive the traps which are checked.

Media Gateway modules and X330WAN expansion modules each have their own trap tables. Managers can be assigned to individual modules and need not receive traps from modules for which they are not responsible.

Viewing the Stack Trap Managers Table

The Stack Trap Managers tables are used to configure the IP addresses of the trap managers and their trap reporting statuses for device wide traps. Traps include power, fan, faults, and module insert/remove traps.

The device has Stack Trap Manager tables supporting both SNMPv1 and SNMPv3 users.

Stack Trap Manager Table - SNMPv1 Legacy Tab

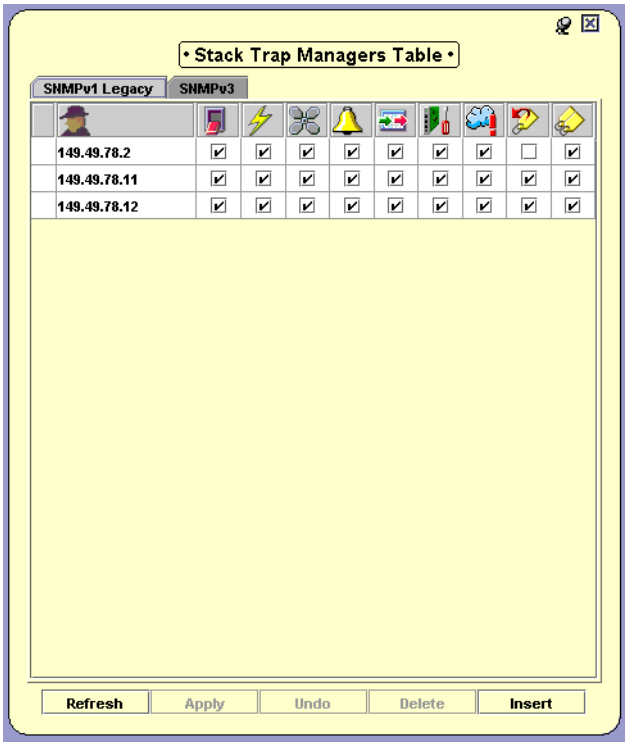
To view the Stack Trap Managers SNMPv1 Legacy tab:

1. Verify that a G700 or X330WAN module is not selected.
2. Click .

   Or

   Select **Configure > Trap Managers**. The Stack Trap Managers Table dialog box opens to the SNMPv1 tab.

Figure 14-1. Stack Trap Managers Table - SNMPv1 Legacy Tab



The following table provides a list of device trap types, their associated icons, and their descriptions.

Table 14-1. Trap Types

Icon	Trap	Description
	Trap Enable	Enables trap reporting for the selected manager.
	Power Supply Traps	The trap reports the failure of a PSU.
	Fan Traps	The trap reports the failure of a fan.
	Fault Traps	A group of traps that report a fault in the device.
	Module Insert Remove Traps	The trap reports the insertion or removal of a module in the device.
	Configuration Changed Traps	A group of traps that report a change in the configuration of the device.
	IP VLAN Violation Traps	The trap reports the reception of a packet tagged with a VLAN ID not equal to the IP interface of the router.

Table 14-1. Trap Types (Continued)

Icon	Trap	Description
	IP Access Control Traps	A trap that reports the arrival of a packet which is assigned not to enter the router.
	Duplicate IP Traps	A trap that reports that a user has configured a device on the network with an IP address that is already being used by the router.

For information on adding and removing trap managers and editing their trap reporting statuses, refer to "Editing the Trap Managers Table" on page 193.

Stack Trap Managers Table - SNMPv3 Tab

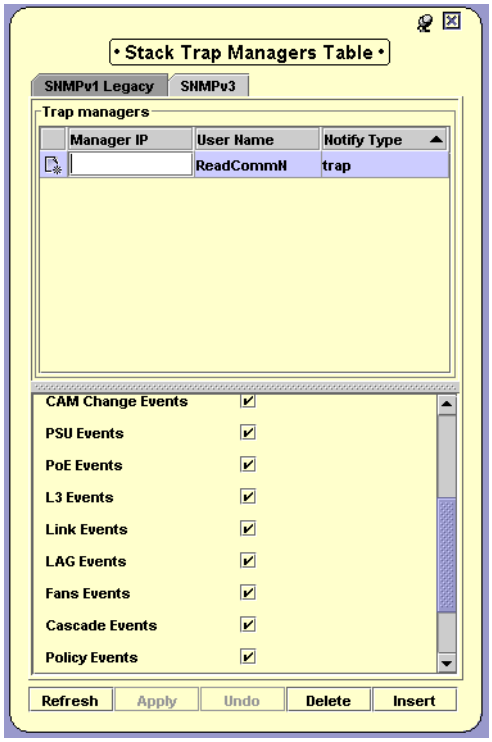
To view the Stack Trap Managers Table SNMPv3 tab:

1. Verify that a G700 or X330WAN module is not selected.
2. Click .

   Or

   Select **Configure > Trap Managers**. The Stack Trap Managers Table dialog box opens to the SNMPv1 Legacy tab.
3. Click **SNMPv3**. The Stack Trap Managers Table dialog box opens to the SNMPv3 tab.

Figure 14-2. Stack Trap Managers Table - SNMPv3 Tab



The following table provides a list of the fields in the SNMPv3 tab of the Stack Trap Manager Table dialog box and their descriptions.

Table 14-2. Stack Trap Manager Options - SNMPv3 Tab

Field	Description
Manager IP	IP address of the destination Trap Manager.
User Name	User name to access the Trap Manager.
Notify Mode	Security model used to send traps to Trap Managers. Possible values are: • SNMPv1 • SNMPv2 • SNMPv3-No Auth • SNMPv3-Auth • SNMPv3-Auth Priv
Inform Timeout	The amount of time in seconds that the device will attempt to contact the Trap Managers. Possible values are 100-10,000.

Table 14-2. Stack Trap Manager Options - SNMPv3 Tab (Continued)

Field	Description
Inform Retry Count	The number of times the device will attempt to send an Inform message to the Trap Managers. Possible values are 1-10.
Config Change Events	When checked, Config Change events are sent to the manager.
SW Redundancy Events	When checked, Software Redundancy events are sent to the manager.
Temperature Events	When checked, Temperature events are sent to the manager.
CAM Change Events	When checked, CAM Change events are sent to the manager.
PSU Events	When checked, PSU events are sent to the manager.
PoE Events	When checked, PoE events are sent to the manager.
L3 Events	When checked, L3 events are sent to the manager.
Link Events	When checked, Link events are sent to the manager.
LAG Events	When checked, LAG events are sent to the manager.
Fans Events	When checked, Fans events are sent to the manager.
Cascade Events	When checked, Cascade events are sent to the manager.
Policy Events	When checked, Policy events are sent to the manager.
Eth Port Fault Events	When checked, Ethernet Port Fault events are sent to the manager.
Security Events	When checked, Security events are sent to the manager.
Generic Events	When checked, Generic events are sent to the manager.

Viewing the Media Gateway Trap Managers Table

To view the Trap Managers table for a G700 Media Gateway:

1. Select the G700 Media Gateway for which you want to view the Trap Managers table.

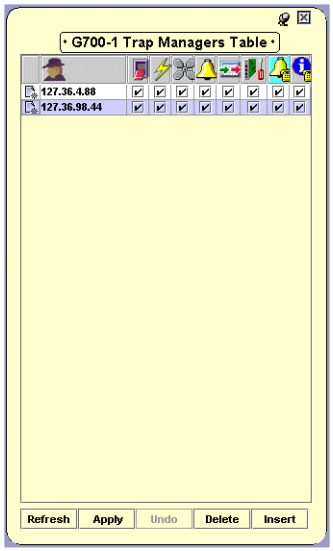
*** Note:** Each G700 Media Gateway module has its own Trap Managers table, which can be used to configure IP addresses and trap managers for the specific module. Device wide trap settings do not apply to traps from G700 Media Gateways in the device.

2. Click .

   Or

   Select **Configure > Trap Managers**. The Media Gateway Trap Managers table opens.

Figure 14-3. Media Gateway Trap Managers Table



The Media Gateway Trap Managers table is used to configure the IP addresses of the trap managers and their trap reporting statuses for Media Gateway traps. Traps include power, fan, faults, module insert/remove, and voice related traps.

To enable RTP QoS traps on the Media Gateway module, check the Enable RTP QoS traps checkbox. To disable frame relay traps on the Media Gateway module, uncheck the Enable RTP QoS traps checkbox.

To enable RTP QoS Fault traps on the Media Gateway module, check the Enable RTP QoS Fault traps checkbox. To disable frame relay traps on the Media Gateway module, uncheck the Enable RTP QoS Fault traps checkbox.

The following table provides a list of trap types, their associated icons, and their descriptions.

Table 14-3. Media Gateway Trap Types

Icon	Trap	Description
	Trap Enable	Enables trap reporting for the selected manager.
	Power Supply Traps	The trap reports the failure of a PSU.
	Fan Traps	The trap reports the failure of a fan.
	Fault Traps	A group of traps that report a fault in the device.
	Module Insert Remove Traps	The trap reports the insertion or removal of a module in the device.
	Configuration Changed Traps	A group of traps that report a change in the configuration of the device.
	Voice Fault Traps	A group of traps that report quality of service problems with the voice hardware.
	Voice Information Traps	A group of traps that report on the normal operation of the Media Gateway.

For information on adding and removing trap managers and editing their trap reporting statuses, refer to "Editing the Trap Managers Table" on page 193.

Viewing the WAN Trap Managers Table

To view the Trap Managers table for an X330WAN expansion module:

1. Select the X330WAN expansion module for which you want to view the Trap Managers table.

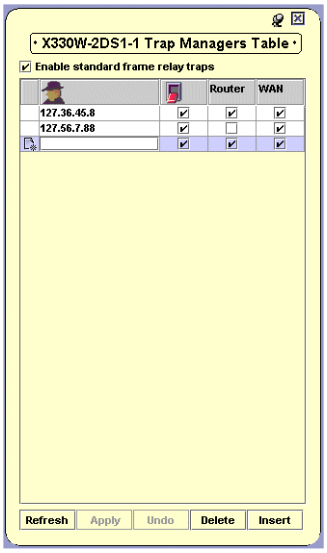
*** Note:** Each X330WAN expansion module has its own Trap Managers table, which can be used to configure IP addresses and trap managers for the specific module. Device wide trap settings do not apply to traps from X330WAN expansion modules in the device.

2. Click .

Or

Select **Configure > Trap Managers**. The WAN Trap Managers table opens.

Figure 14-4. WAN Trap Managers Table



The WAN Trap Managers table is used to configure the IP addresses of the trap managers and their trap reporting statuses for WAN traps. Traps include routing, WAN, and frame relay traps.

Frame relay traps can only be enabled or disabled per X330WAN expansion module. If frame relay traps are enabled, all enabled managers receive frame relay traps. If frame relay traps are disabled, no managers will receive frame relay traps.

To enable frame relay traps on the X330WAN expansion module, check the Enable standard frame relay traps checkbox. To disable frame relay traps on the X330WAN expansion module, uncheck the Enable standard frame relay traps checkbox.

The following table provides a list of trap types, their associated icons, and their descriptions.

Table 14-4. WAN Trap Types

Icon	Trap	Description
	Trap Enable	Enables trap reporting for the selected manager.
	Router Traps	A group of traps that report router detected events.
	WAN Traps	A group of traps that report problems with the WAN interface and cable.

For information on adding and removing trap managers and editing their trap reporting statuses, refer to "Editing the Trap Managers Table" on page 193.

Editing the Trap Managers Table

You can add and remove managers from the Trap Managers table, and you can edit the trap reporting status of specific managers.

Adding and Removing Managers

To add managers to the table:

1. Click **Insert**.
2. Enter the IP address of the designated management station.
3. Repeat the procedure for each manager.

To remove managers from the table:

1. Click the row with the manager's IP address.
2. Click **Delete**.
3. Repeat the procedure for each manager.

Editing Trap Reporting Statuses

To edit the trap reporting status of a manager, check or uncheck the checkboxes next to the manager's IP address.

Checked traps will be reported to the manager.

*** Note:** If the Trap Enable checkbox is not checked, no traps will be reported to the selected manager.

For more information on the user interface, refer to "Using Dialog Boxes and Tables" on page 16.

For more information on tables, refer to "Managing Tables" on page 5.

15 Switch Connected Addresses

This chapter provides the information and instructions for viewing stations connected to the device. It includes the following topics:

- **Switch Connected Addresses Overview** - An overview of the Switch Connected Addresses feature.
- **Viewing the Switch Connected Addresses Window** - Instructions on accessing the Switch Connected for Device window, and a description of the Switch Connected for Device window.

Switch Connected Addresses Overview

The Switch Connected Addresses feature allows you to see which devices are connected to the ports on the Avaya C360 Device. Keeping track of this network information can increase efficiency and security, and assist in troubleshooting network problems.

Viewing the Switch Connected Addresses Window

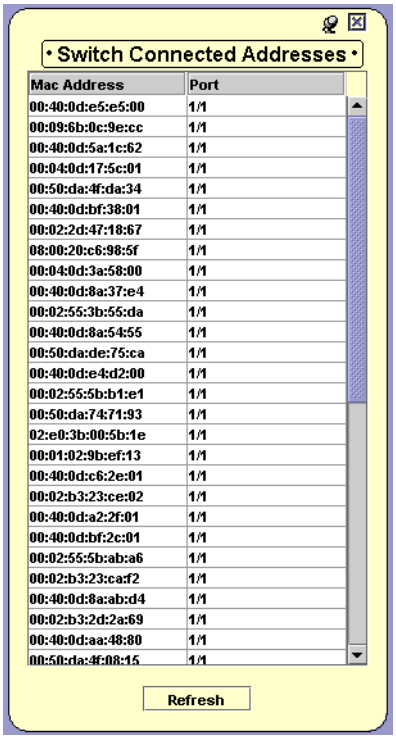
The Switch Connected Addresses window provides a list of MAC addresses along with the ports to which they are attached. To view the list of connected stations:

Click .

Or

Select **View > Switch Connected Addresses**. The Switch Connected Addresses window opens.

Figure 15-1. Switch Connected Addresses Window



All the connections to the Avaya C360 are listed with their respective ports in the Switch Connected Addresses window. The rows of the Switch Connected Addresses window comprise the following information:

- **Mac Address** - The MAC addresses of the stations connected to the switch.
- **Port** - The number of the module and port in the switch.

To refresh the information in the Switch Connected Addresses window, click **Refresh**.

Sorting the List of Stations

To sort the list of stations, click on a column heading to sort by that column. To change the order of the sort (e.g. from ascending to descending), click the column heading of the field by which the list is sorted.

For more information on the user interface, refer to "Using Dialog Boxes and Tables" on page 16.

16 Port Security

This chapter provides the information and instructions you need to use port security with Avaya C360 ports.

Port security enables you to prevent unauthorized users and devices from sending information through the ports in your network. The following method of port security is available for Avaya C360 ports:

- **802.1x Port Security**
- **MAC Port Security**

802.1x Port Security

This section provides information and instructions about using the 802.1x port security feature. It includes the following topics:

- **802.1x Port Security Overview** - An overview of 802.1x port security.
- **Configuring 802.1x Port Security** - Instructions on how to configure 802.1x port security.

802.1x Port Security Overview

802.1x port security requires a user connected to a port in the network to be authenticated by an authentication server.

When a user connects to a port configured with 802.1x port security, the port forwards an authentication request to a RADIUS authentication server. The authentication server checks if the user is authorized to use the port, and either allows or blocks access to the port.

The port can be configured to reauthenticate the user. If the reauthentication fails, the user is denied further access to the port.

Configuring 802.1x Port Security

To configure 802.1x port security for a selected port:

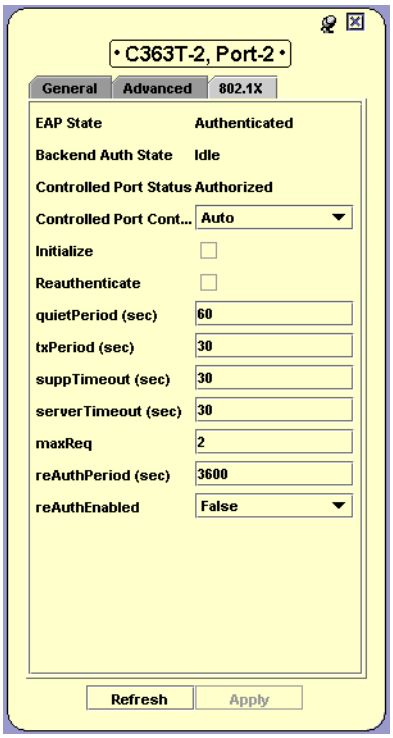
1. Click the port symbol in the Chassis View.

   Or

   Click the port's icon in the Tree View. The Port Configuration dialog box opens to the General tab.

2. Click **802.1x**. The 802.1x tab of the Port Configuration dialog box appears.

Figure 16-1. Port Configuration Dialog Box - 802.1x Tab



3. Configure the port's 802.1x port security configuration using the fields in the 802.1x tab of the Port Configuration dialog box.

The following table provides a list of the fields in the 802.1x tab of the Port Configuration dialog box and their descriptions:

Table 16-1. Port Configuration Fields - 802.1x Tab

Field	Description
EAP State	The Entity Access Port state. Possible states include: • **Initialize** • **Disconnected** • **Connecting** • **Authenticating** • **Authenticated** • **Aborting** • **Held** • **ForceAuth** • **ForceUnauth**
Backend Auth State	The current state of the Backend Authentication state machine. Possible states include: • **Request** • **Response** • **Success** • **Fail** • **Timeout** • **Idle** • **Initialize**
Controlled Port Status	The current value of the controlled port status. Possible states include: • **Authorized** • **Unauthorized**
Controlled Port Control	The current value of the controlled port control. Possible states include: • **ForceAuthorized** • **ForceUnauthorized**
Initialize	Forces initialization of the port. Checking the Initialize checkbox and clicking **Apply** forces the port to be initialized immediately

Table 16-1. Port Configuration Fields - 802.1x Tab (Continued)

Field	Description
Reauthenticate	Forces a reauthentication. Checking the Reauthentication checkbox and clicking **Apply** forces the user to be reauthenticated immediately.
quietPeriod (sec)	The amount of time, in seconds, between sending authentication requests.
txPeriod (sec)	The amount of time, in seconds, in which an authentication request must be answered.
suppTimeout (sec)	The amount of time, in seconds, before resending authentication requests.
serverTimeout (sec)	The amount of time, in seconds, before timing out an authentication request
maxReq	The maximum number of times a request for authentication is sent before timing out.
reAuthPeriod (sec)	The time, in seconds, after which the port connection should be reauthenticated.
reAuthEnabled	The state of reauthentication on the port. Possible states include: • **True** - The port connection is reauthenticated after the reAuthPeriod. • **False** - The port connection is not reauthenticated. The reAuthPeriod is ignored.

For more information on the user interface, refer to "Using Dialog Boxes and Tables" on page 16.

The Get/Set Toolbar provides an alternative, quick method to view and change the port's 802.1x configuration. For more information on the Get/Set Toolbar, refer to "Get/Set Toolbar" on page 10.

MAC Port Security

This section provides information and instructions about using the MAC Port Security feature. It includes the following topics:

- **MAC Port Security Overview** - An overview of MAC Port Security.
- **Configuring MAC Port Security** - Instructions on how to configure MAC Port Security.

*** Note:** In the C360, MAC Security implementation applies specifically to the 10/100 BaseT and SFP/Giga ports.

MAC Port Security Overview

The MAC Port Security function is intended to filter incoming frames with an unauthorized source MAC address (SA) on a secured port.

When a frame is received on a secured port, its SA is checked against the MAC Address Table. If the SA is not found in the MAC Address Table or it is found but has a different port location than the incoming frame, the frame is rejected without being learned. A message is then sent to the Agent.

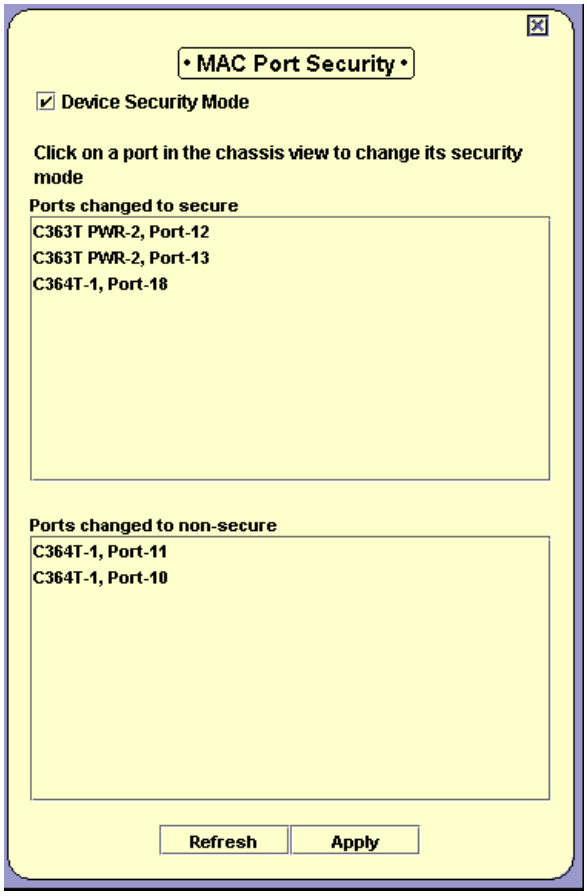
The Agent reports the attempted intrusion with an SNMP security violation trap containing the intruder's MAC address. To prevent the flooding of the Console's trap log or network, the Agent sends an intruder alert every 5 seconds for the first 3 times a specific intruder is detected on a port, and then every 15 minutes if the intrusion continues.

Configuring MAC Port Security

To apply MAC Port Security to a selected port:

1. Select **Configure > MAC Port Security**. The MAC Port Security dialog box opens.

Figure 16-2. MAC Port Security Dialog Box



2. Check the **Device Security Mode** check box.
3. In chassis view, click on the port you want to secure. The port will appear in the Ports changed to secure list.
4. Click **Apply**.

To remove MAC Port Security from a previously secured port:

1. Select **Configure > MAC Port Security**. The MAC Port Security dialog box opens.
2. In chassis view, click the port you want to unsecure. The port appears in the Ports changed to non-secure list.
3. Click **Apply**.

The following table provides a list of the fields in the MAC Port Security dialog box and their descriptions:

Table 16-2. MAC Port Security Parameters

Field	Description
Device Security Mode	When checked, the device is configured to use MAC Port Security for selected ports.
Ports changed to secure	Lists the ports to which MAC Port Security is applied.
Ports changed to non-secure	Lists previously secured ports from which MAC Port Security has been removed.

17 Routing Manager

This chapter provides an introduction to the Avaya C360 Routing Manager. It includes the following sections:

- **Router Modes** - An introduction to the different modes of the Avaya C360 Router.
- **The User Interface** - An introduction to the Avaya C360 Routing Manager user interface.
- **Editing Tables** - An explanation of how to edit Avaya C360 Routing Manager tables.
- **Saving Table Information as Text** - Instructions on how to save the information in a table to a text file.
- **Saving Configuration Changes** - An explanation of how to apply and save configuration changes to routers.
- **Resetting a Router** - Instructions on how to reset routers.
- **Using Avaya C360 Routing Manager Help** - An explanation of the options for accessing on-line help in the Avaya C360 Routing Manager.

Router Modes

The Avaya P330ML and C360 modules, and Avaya X330WAN expansion module provide routing capabilities in an Avaya C360 Stack. The Avaya C360 module can be configured with one of the following routing modes:

- **Router**
- **Layer 2 Switch**

The default mode is Router. For information on changing the routing mode, refer to "Viewing Module Configuration" on page 24.

*** Note:** The Avaya X330WAN expansion module always operates in Router mode.

Router

When configured with the Router mode, the Avaya C360 is a fully configurable router.

Layer 2 Switch

When the Avaya C360 routing mode is configured as a Layer 2 Switch, the module performs no routing functions.

The User Interface

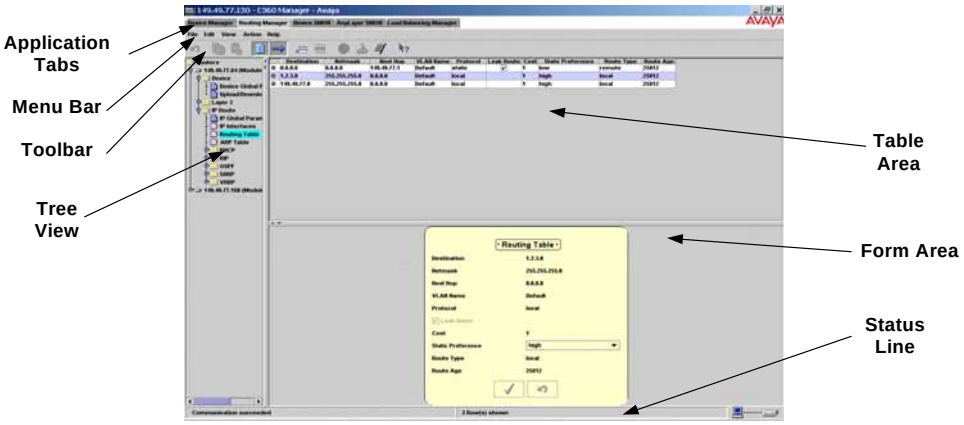
The user interface consists of the following elements:

- **Toolbar** - A toolbar providing shortcuts to the main Routing Manager functions.
- **Tree View** - A resizeable window containing a hierarchical representation of the router modules in the device and configuration windows of Avaya C360 Routing Configuration.
- **Table Area** - A resizeable window where all tables are displayed.
- **Form Area** - A resizeable window where all forms appear.

For information on other parts of the user interface, refer to "The User Interface" on page 4.

The figure below shows the user interface, with its various parts labeled.

Figure 17-1. Avaya C360 Routing Manager User Interface



To resize the main areas of the user interface, the Tree View, the Table Area, and the Form Area, use the splitter bars and their arrows.

Toolbar

The Toolbar provides shortcuts to the main Routing Manager functions.

The table below describes the buttons on the Application Toolbar and gives the equivalent menu options.

Table 17-1. Application Toolbar

Button	Description	Menu Item
	Undoes changes made to the table or form currently displayed.	**Edit > Undo**
	Copies the selected information to the clipboard.	**Edit > Copy**
	Pastes information from the clipboard into the selected table row.	**Edit > Paste**
	Toggles the display of a form corresponding to the current table.	**View > Form**
	Toggles the display of additional table parameters.	**View > More**
	Adds a row to the table.	**Edit > Insert Row**
	Deletes the selected table row.	**Edit > Delete Row**
	Stops loading information into the current table.	**Action > Stop**
	Sends the configuration information to the device.	**Action > Apply**
	Opens a dialog box which enables you to specify the starting point in the display of a table.	**Action > Start Point**
	Opens the on-line help for context-sensitive information.	**Help > Context Sensitive Help**

Tree View

The Tree View shows the Avaya P330ML and C360 modules, and X330WAN expansion modules in the device and the applicable configuration windows for each module.

The highest level of the Tree View shows the device's router modules. Each module that is configured as a router is shown. The second and third levels show the configuration windows applicable to the modules.

To expand the view of a contracted element in the tree or to contract the view of an expanded element in the tree:

Double-click the element.

Or

Click the handle next to the element you want to expand or contract.

Table Area

The right side of the application window is the Table Area. This area can be resized by dragging the vertical splitter bar with the mouse. All tables appear in the Table Area. Table columns can be resized by dragging the dividers in the table header.

To view additional parameters in the table:

Click .

Or

Open Select **View > More**. Additional parameters appear in the table.

To hide additional parameters in the table:

Click .

Or

Select **View > More**. Additional parameters do not appear in the table.

Form Area

The area at the bottom of the Table Area is where all forms appear. This area can be resized by dragging the horizontal splitter bar with the mouse. When a form opens, it replaces the current form open in the Form Area.

Tables have associated forms that can be used to edit the information in a table row or insert information into a new table row.

To toggle the display of forms associated with table rows:

1. Select a table row.
2. Click .

   Or

   Select **View > Form**. The display of the associated form is toggled.

Editing Tables

The Avaya Routing Manager user interface enables you to create, modify, and delete table entries in selected windows. The information can be added directly into the table, or in the form associated with the table.

To undo all the changes made to a table, click . When all changes are finalized, click to update the router.

Creating New Table Entries

To create a new table entry:

1. Click .

   Or

   Select **Edit > Insert Row**. A new table entry is created.

2. Enter data in the fields as required.
3. Click to update the router.

Modifying Table Entries

To modify data in table entries:

1. Select the table entry you want to modify by clicking it.
2. Click a field.
3. Modify the value of the selected parameters.
4. When you are finished editing the table, click to update the router.

Deleting Table Entries

To delete a table entry:

1. Select the table entry you want to delete by clicking it.
2. Click .

   Or

   Select **Edit > Delete Row**. The selected entry is deleted from the table.

3. Click to update the router.

Saving Table Information as Text

Information in tables can be saved to text files. To save the information in the current table to a text file:

1. Select **File > Save**. The File Save dialog box opens.
2. Use the browser to select a directory.
3. Enter a filename in the File name field.
4. Click **Save**. The information is saved as a text file to the specified file.

Saving Configuration Changes

There are two levels of applying routing configuration changes to the router:

- **Running Changes** - Changes are applied to the router, but are not saved.
- **Committed Changes** - Changes are saved to the router.

Running Changes

After finalizing all changes to a dialog box or table, the changes must be sent to the router. To send the changes to the router, click . The configuration changes are applied to the router.

The changes remain in effect until the router is reset. When the router is reset, it is configured with the last saved configuration. All changes applied but not saved are lost.

Committed Changes

To make configuration changes permanent, the changes must be committed (saved) to the router. To commit the configuration to the router, select **File > Commit**. The changes are committed to the router.

Resetting a Router

To reset a router:

1. Click the router's icon in the Tree View.
2. Select **Action > Reset**. A confirmation dialog box opens.
3. Click **Yes**. The selected router is reset.

Using Avaya C360 Routing Manager Help

This section explains how to use the on-line help in the Avaya C360 Routing Manager. The on-line help can be opened to the contents page or directly to a topic of interest.

*** Note:** When running the Avaya C360 Manager via Web Management, on-line help is only available if you have installed the on-line help on your network and configured the Avaya C360 Device with the location of the help files. For information on installing the on-line help and configuring the device with the location of the files, refer to the *Avaya C360 User's Guide*.

Opening the Help to the Contents Page

To open the help to the contents page, select **Help > Contents**. The on-line help opens to the contents page.

Opening the Help to a Topic of Interest

To open the help directly to a topic of interest, click . The on-line help opens to a topic explaining the option currently selected in the Tree View.

18 Device

The Device folder provides access to the following windows:

- **Device Global Parameters**

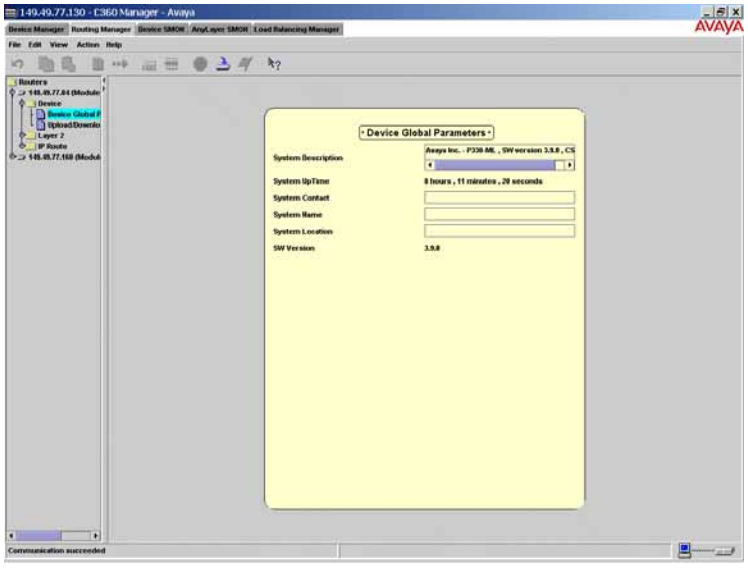
*** Note:** When configuring an Avaya X330WAN router, there is no Device Global Parameters window.

Device Global Parameters

*** Note:** When configuring an Avaya X330WAN router, there is no Device Global Parameters window.

To display and update global device parameters, select **Device > Device Global Parameters**. The Device Global Parameters window opens.

Figure 18-1. Device Global Parameters Window



The following parameters are displayed:

Table 18-1. Global Parameters

Field	Description
System Description	A general description of the device.
System UpTime	The time elapsed since the device was reset.
System Contact	The name of the person responsible for the device.
System Name	The user-assigned name of the device that appears in the windows describing the device.
System Location	The location of the device.
Primary Management Interface (X330WAN only)	The IP address of the router's main interface.
SW Version	The software version of the code on the device (for example, 2.5.7).

You can edit the System Contact, System Name, and System Location fields.

19 Layer 2

The Layer 2 folder provides access to the following window:

- VLANs

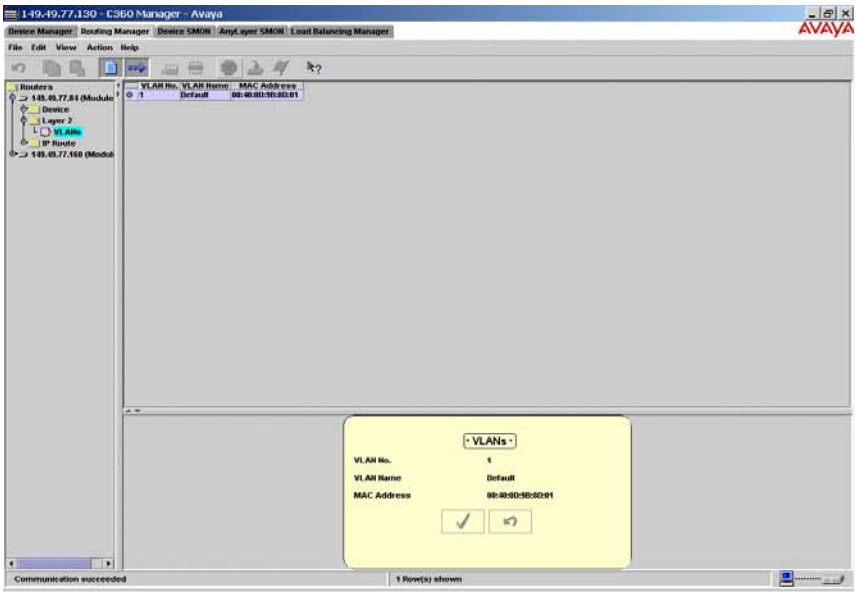
*** Note:** When configuring an Avaya X330WAN router, the Layer 2 folder provides access to the **L2 Interfaces** window.

VLANs

*** Note:** When configuring an Avaya X330WAN router, this window is called the **L2 Interfaces** window.

To display the layer 2 interfaces, select **Layer 2 > VLANs**. The VLANs window opens.

Figure 19-1. VLANs Window



The following parameters are displayed:

Table 19-1. VLANs Window Parameters

Field	Description
VLAN No. (not for X330WAN router)	The VLAN number of this VLAN.
Interface No. (X330WAN router only)	The number of this layer 2 interface.
VLAN Name (not for X330WAN router)	The VLAN name of this VLAN.
Interface Name (X330WAN router only)	The logical name of this layer 2 interface.
MAC Address	The MAC address of this VLAN or layer 2 interface.
Peer Address (X330WAN router only)	The IP address of the interface's peer.
Oper Status (X330WAN router only)	The operational status of this layer 2 interface.

The fields in the VLANs window are read-only.

20 IP Route

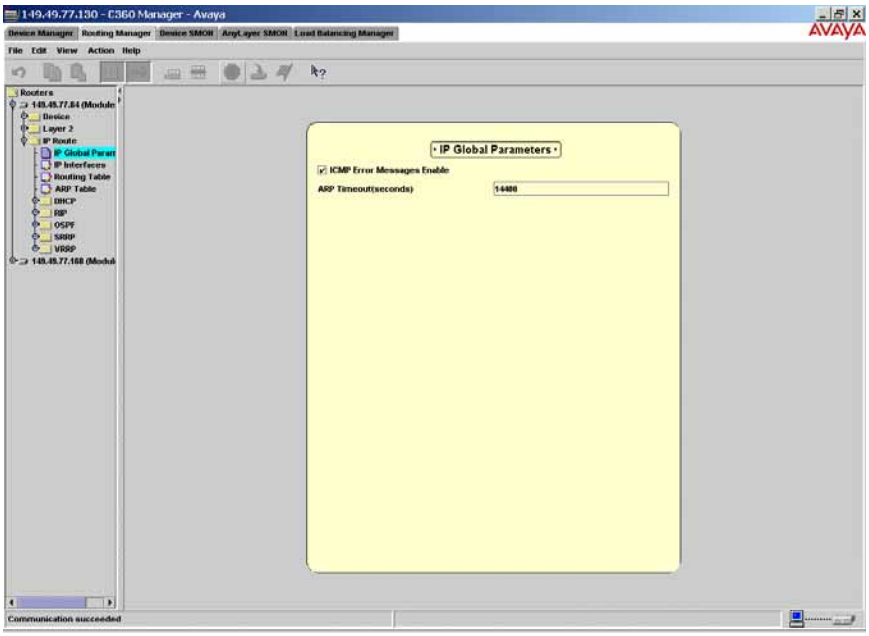
The IP Route folder provides access to the following windows:

- **IP Global Parameters**
- **IP Interfaces**
- **Routing Table**
- **ARP Table**
- **DHCP**
- **RIP**
- **OSPF**
- **VRRP**
- **CRTP**

IP Global Parameters

To display and update the IP global parameters, select **IP Route > IP Global Parameters**. The IP Global Parameters window opens.

Figure 20-1. IP Global Parameters Window



The following parameters are displayed:

Table 20-1. IP Global Parameters

Field	Description
ICMP Error Messages Enable	If checked, ICMP error messages should be sent. If not checked, ICMP error messages should not be sent.
ARP Timeout (seconds)	The number of seconds that may pass between ARP requests concerning entries in the ARP table. After this period, the entry is deleted from the table.

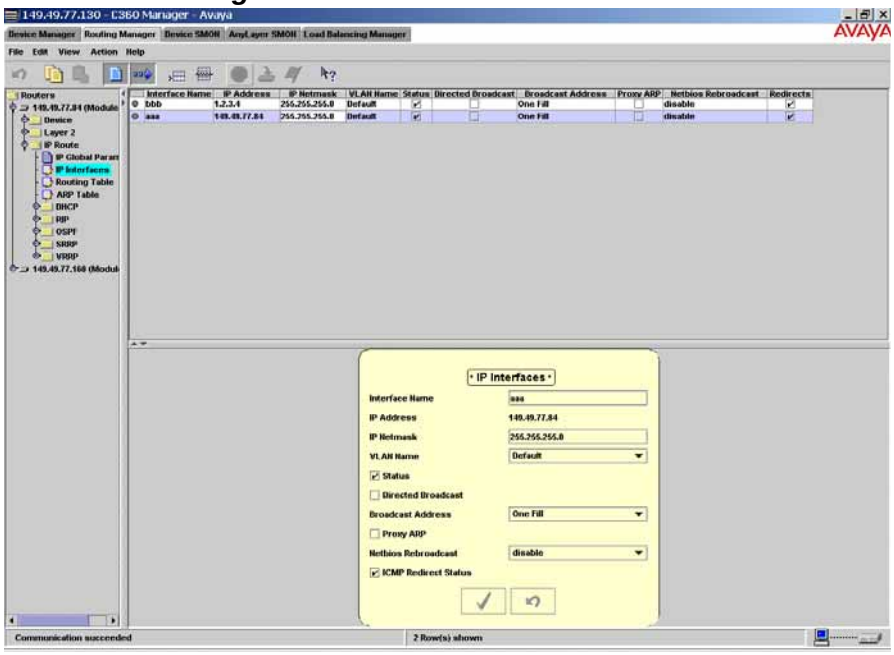
IP Interfaces

IP interfaces represent the logical connections of the device to the IP nets/subnets attached to it. Each IP interface corresponds to one net/subnet.

When you create a new IP interface, RIP and OSPF interfaces are automatically created and assigned enable status. When you delete an IP interface, the device deletes the associated RIP and OSPF interfaces.

To define and display the IP interfaces, select **IP Route > IP Interfaces**. The IP Interfaces window opens.

Figure 20-2. IP Interfaces WIndow



The following parameters are displayed:

Table 20-2. IP Interface Table Parameters

Field	Description
Interface Name (not for X330WAN router)	The name assigned to the selected IP interface.
IP Interface Name (X330WAN router only)	The name assigned to the selected IP interface.
IP Address	The IP address assigned to the device on this subnet.

Table 20-2. IP Interface Table Parameters (Continued)

Field	Description
IP NetMask	The IP network mask of the attached net/ subnet.
VLAN Name (not for X330WAN router)	The name of the Layer 2 interface with which this subnet is associated. Multiple subnets may be associated with a single VLAN, so multiple IP interfaces may be associated with the same If Name.
L2 Interface Name (X330WAN router only)	The name of the Layer 2 interface with which this subnet is associated. Multiple subnets may be associated with a single interface, so multiple IP interfaces may be associated with the same If Name.
Status	The status of the IP interface. If checked, the IP interface is enabled.
Directed Broadcast	The status of the forwarding of incoming net-directed broadcasts to this interface. If checked, the forwarding is enabled. If not checked, IP directed broadcast messages destined to this interface will be discarded and will not be forwarded to this interface.
Broadcast Address	Determines the format of IP broadcast messages generated by the device. Possible formats are: • **One fill** - The host ID in the broadcast address is filled with 'one' bits (e.g., 149.49.50.255). • **Zero fill** - The host ID in the broadcast address is filled with 'zero' bits (e.g., 149.49.50.0).
Proxy ARP	If checked, the device will respond with its own MAC address to ARP requests for stations that are on another VLAN.
NetBios Rebroadcast	The state of NetBios Rebroadcast on this interface. Possible values are: • **both** - NetBios are rebroadcast both to and from this interface. • **disable** - NetBios are not rebroadcast to or from this interface.

Table 20-2. IP Interface Table Parameters (Continued)

Field	Description
ICMP Redirect Status	The state of ICMP message redirection on the interface. Possible states are: • **enable** - ICMP redirect messages are enabled on this interface. • **disable** - ICMP redirect messages are disabled on this interface.

You can create, modify, and delete IP interfaces. For more information on editing tables, refer to "Editing Tables" on page 213.

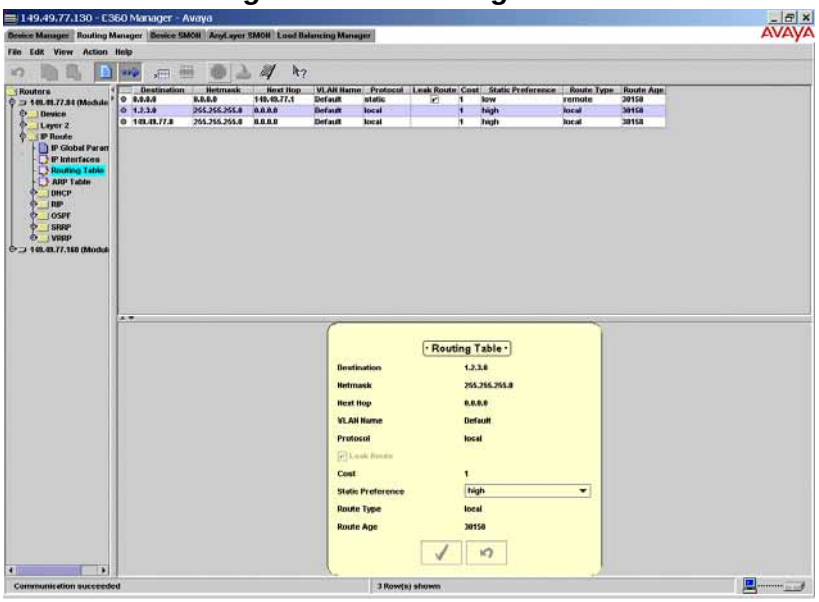
*** Note:** The IP Address, IP NetMask, If Name, and Status must be defined before creating an IP interface.

*** Note:** The list of VLANs allocated in the system is displayed in the If Name field.

Routing Table

To display and update the Routing Table, select **IP Route > Routing Table**. The Routing Table window opens.

Figure 20-3. Routing Table



The following parameters are displayed:

Table 20-3. Routing Table Parameters

Field	Description
Destination	The destination network IP address of this route. An IP address of 0.0.0.0 denotes a default router.
Netmask	The destination network mask of this route.
Next Hop	The address of the next router of this route, via which the destination of this route is reached.
VLAN Name (not for X330WAN)	The logical name of the local interface through which the next hop of this route is reached.
L2 Interface Name (X330WAN router only)	The logical name of the local interface through which the next hop of this route is reached.
Protocol	The protocol through which the route was learned. The following protocols can be specified: • **Static** - The route was manually configured to this device. • **Local** - The route represents a directly attached net/subnet and corresponds to one of the IP interfaces configured to this device. • **RIP** - The entry was learned from the RIP protocol. • **OSPF** - The entry was learned from the OSPF protocol.
Leak Route	If checked, static entries are advertised by RIP and OSPF. If unchecked, static entries are not advertised.
Cost	Number of hops to the destination network, or the cost of the route for OSPF routes.
Permanent (X330WAN router only)	The permanence status of the route. Possible statuses are: • **Checked** - The route is not disabled when a link on the route is down. • **Unchecked** - The route is disabled when a link on the route is down.

Table 20-3. Routing Table Parameters (Continued)

Field	Description
Static Preference	The preference of this route. Possible values are: • **low** - Dynamic routes are preferred on this static route. • **high** - This static route is preferred on dynamic routes.
Route Type	The type of route, either local or remote.
Route Age	The number of seconds since the route was last updated.

You can create, modify, or delete Routing Table static entries. For more information on editing tables, refer to "Editing Tables" on page 213.

*** Note:** Only static entries in the Routing Table can be modified. Entries learned from OSPF, RIP, or local cannot be modified.

When adding Routing Table entries on an Avaya X330WAN router, you can configure the next hop method in the Form View. Available next hop methods include:

- **Next Hop** - Select the **Next Hop** option button, and enter the IP address of the next hop.
- **L2 Interface Name** - Select the **L2 Interface Name** option button, and select an interface from the pull-down listbox.
- **Discard** - Select the **Discard** option button.

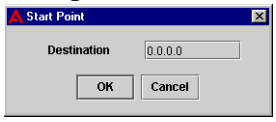
You can limit the table entries displayed. To start the display of entries from a specified interface and IP address:

1. Click .

   Or

   Select **Action > Start Point**. The Start Point dialog box opens.

Figure 20-4. Routing Table Start Point Dialog Box



2. Enter an IP address in the Destination field.
3. Click **OK**. The Routing Table displays entries starting with the specified IP address.

To view all the entries in the Routing Table:

Click .

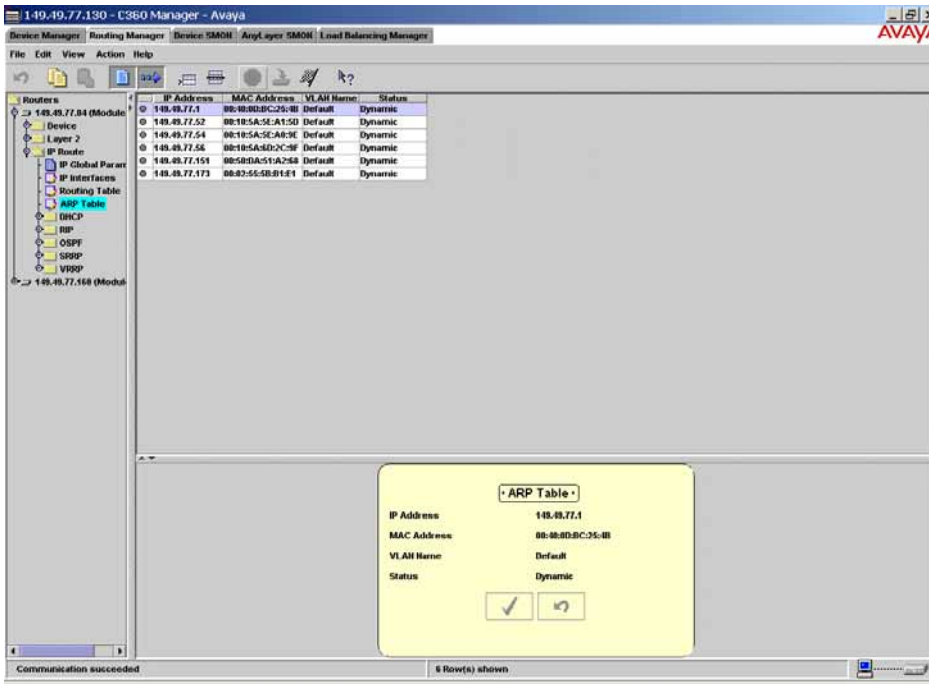
Or

Select **View > Refresh**. All entries appear in the table.

ARP Table

To display and update the ARP Table parameters, select **IP Route > ARP Table**. The ARP Table window opens.

Figure 20-5. ARP Table Window



The following parameters are displayed:

Table 20-4. ARP Parameters

Field	Description
IP Address	The IP address of the station.
MAC Address	The MAC address of the station.
VLAN Name (not for X330WAN)	The name of the interface.
L2 Interface Name (X330WAN router only)	The name of the interface.

Table 20-4. ARP Parameters (Continued)

Field	Description
Status	The status of the interface. Possible status values are: • **Dynamic** - The entry is learned from the ARP protocol. If the station entry is not active for a predetermined time, the entry is deleted from the table. • **Static** - The entry has been configured by the network management station and is permanent. • **Invalid** - The entry in the table is invalid.

You can create or delete ARP table entries. For more information on editing tables, refer to "Editing Tables" on page 213.

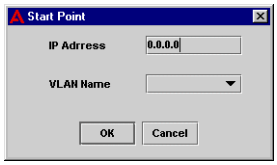
You can limit the table entries displayed. To start the display of entries from a specified interface and IP address:

1. Click .

   Or

   Select **Action > Start Point**. The Start Point dialog box opens.

Figure 20-6. ARP Table Start Point Dialog Box



2. Enter an IP address in the IP Address field.
3. Select an interface from the If Name listbox.
4. Click **OK**. The ARP Table displays entries starting with the specified IP address and interface.

To view all the entries in the ARP Table:

Click .

Or

Select **View > Refresh**. All entries appear in the table.

DHCP

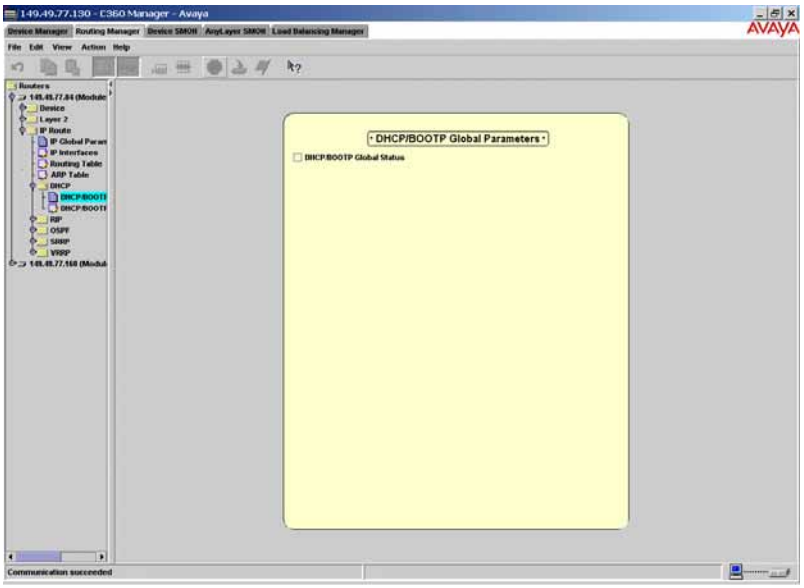
The DHCP folder provides access to the following windows:

- **DHCP/BOOTP Global Parameter**
- **DHCP/BOOTP Parameters**

DHCP/BOOTP Global Parameter

To display and update the DHCP/BOOTP global parameters, select **IP Route > DHCP > DHCP/BOOTP Global Parameters**. The DHCP/BOOTP Global Parameters window opens.

Figure 20-7. DHCP/BOOTP Global Parameters Window



The following parameter is displayed:

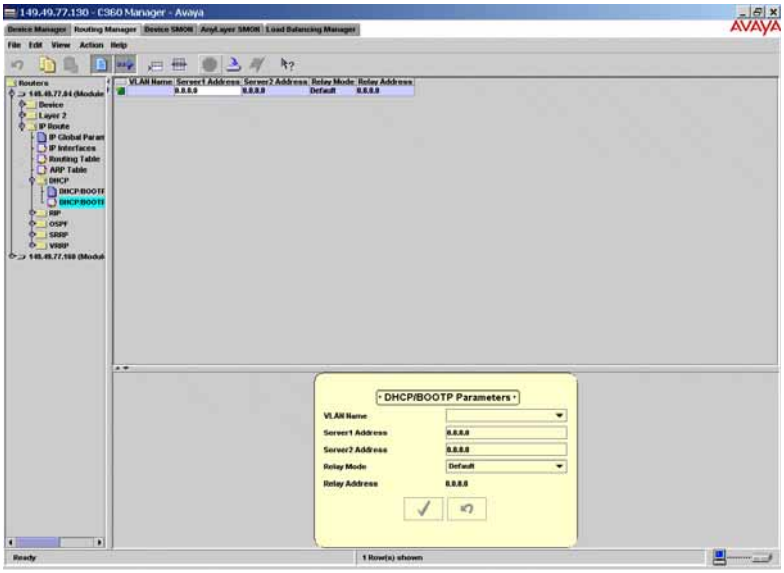
Table 20-5. DHCP/BOOTP Global Parameter

Field	Description
DHCP/BOOTP Global Status	If the DHCP/BOOTP Global Status checkbox is checked, DHCP/BOOTP is enabled according to the DHCP/BOOTP configuration of each interface. If it is not checked, DHCP/BOOTP relays over all interfaces are disabled.

DHCP/BOOTP Parameters

To display and update DHCP/BOOTP parameters, select **IP Route > DHCP > DHCP/BOOTP Parameters**. The DHCP/BOOTP Parameters window opens.

Figure 20-8. DHCP/BOOTP Parameters Window



The following parameters are displayed:

Table 20-6. DHCP/BOOTP Parameters

Field	Description
VLAN Name (not for X330WAN)	The interface name upon which the clients are located.
L2 Interface Name (X330WAN router only)	The interface name upon which the clients are located.
Server1 Address	The IP address of the first of two possible DHCP servers for the interface.
Server2 Address	The IP address of the second of two possible DHCP servers for the interface.

Table 20-6. DHCP/BOOTP Parameters (Continued)

Field	Description
Relay Mode	The method by which the DHCP relay chooses an IP address to include in the DHCP request. When relaying a DHCP/BOOTP request, the relay has to write its own IP address into the relayed DHCP request. This address is used by the DHCP server to determine the subnet from which the client's IP address has been allocated. When the router has multiple IP addresses on the same VLAN, any of these addresses can be used when relaying DHCP requests. The Mode field controls the behavior of the DHCP relay in choosing the IP address to write into the DHCP request. Possible modes are: • **Default** - The router chooses one of the addresses itself. The address chosen will be the lowest IP address on that VLAN. • **Specific** - The router is configured with a single IP address to be used with all relayed requests arriving on the VLAN. This address must be one of the router's IP addresses on the specified VLAN. It must be entered in the Relay Address field.
Relay Address	One of the router's IP addresses on the VLAN. This is used for all relayed requests, if Mode is set to **Specific**.

You can create, modify, or delete DHCP/BOOTP parameters. For more information on editing tables, refer to "Editing Tables" on page 213.

RIP

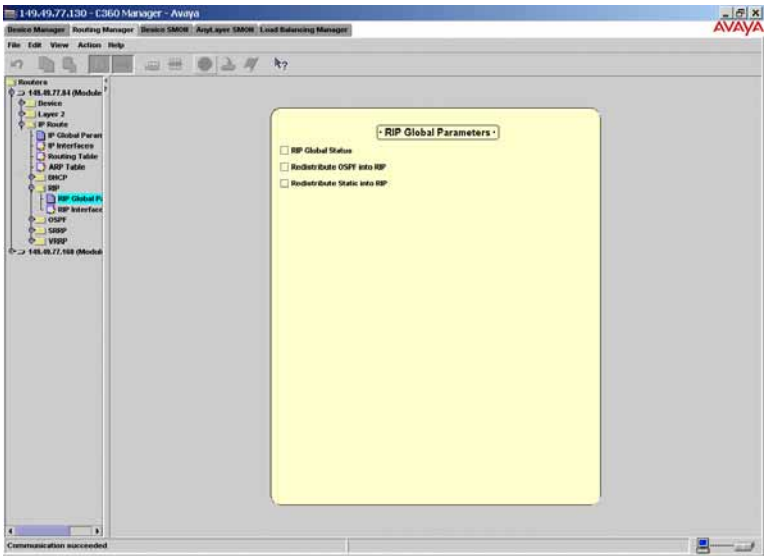
The RIP folder provides access to the following windows:

- **RIP Global Parameters**
- **RIP Interfaces**

RIP Global Parameters

To display and update RIP global parameters, select **IP Route > RIP > RIP Global Parameters**. The RIP Global Parameters window opens.

Figure 20-9. RIP Global Parameters Window



The following parameters are displayed:

Table 20-7. RIP Global Parameters

Field	Description
RIP Global Status	The status of RIP on the device. If checked, RIP is enabled. If not checked, RIP is disabled on all interfaces, regardless of the settings in the RIP Interfaces window.
Redistribute OSPF into RIP	Controls redistribution of routes from OSPF to RIP. If checked, all routes learned via OSPF are advertised into RIP.

Table 20-7. RIP Global Parameters (Continued)

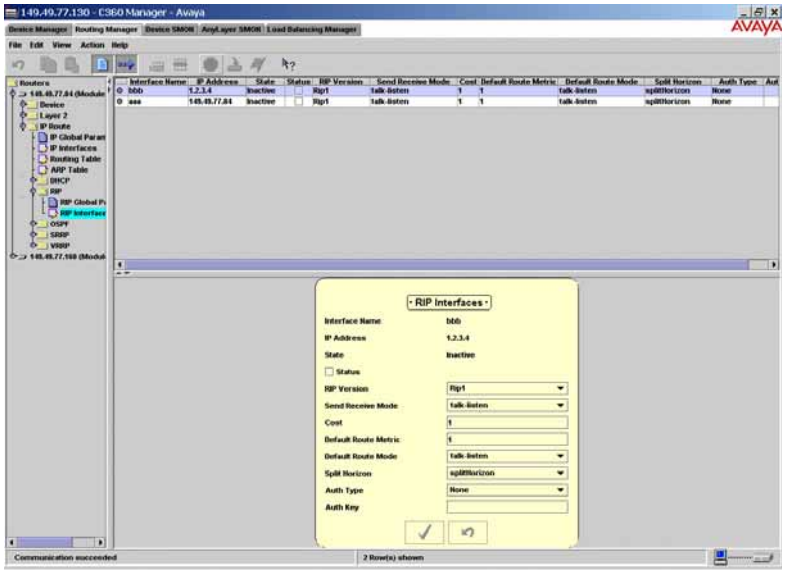
Field	Description
Redistribute Static into RIP	Controls redistribution of static routes into RIP. If checked, the static routes inserted into the IP Routing Table are advertised into RIP, according to the "Leak Route" definition for each static route.
Update Interval (seconds) (X330WAN router only)	The amount of time between each RIP periodic update.
Route Invalidate Timeout (seconds) (X330WAN router only)	The amount of time after which a route becomes invalid in the routing table.

You can modify RIP Global Parameters by checking boxes as desired.

RIP Interfaces

To define and display RIP interfaces, select **IP Route > RIP > RIP Interfaces**. The RIP Interfaces window opens.

Figure 20-10. RIP Interfaces Window



The following parameters are displayed:

Table 20-8. RIP Interface Parameters

Field	Description
Interface Name	The name assigned to the selected IP interface.
IP Address	The IP address of the interface.
State	The operational status of the RIP interface - active or inactive.
Status	The administrative status of the RIP interface. If checked, the RIP interface status is enabled. If unchecked, it is disabled.

Table 20-8. RIP Interface Parameters (Continued)

Field	Description
RIP Version	The router can be configured to operate either RIP version 1 or RIP version 2 on each IP interface. The configuration of the RIP version must be consistent on each subnet. That is, all routers should be configured with the same RIP version on their interface to the subnet. When possible, homogeneous configuration of the RIP version in the network is recommended. • **Rip1** - The router runs regular RIP on that interface, following the RIP version 1 subnet aggregation rules. That is, it advertises an aggregate route for the net as opposed to advertising subnet routes across the network boundary. • **Rip2** - The router runs RIP version 2 on that interface. RIP version 2 advertisements are sent as multicast rather than broadcast. No route aggregation is done in RIP version 2. RIP version 2 allows for Variable Length Subnets Masks (VLSM), meaning that subnets of the same net may have masks of different lengths, and may be of different sizes.
Send Receive Mode	What the device sends on this interface. Values are: • **talk-listen** - RIP updates contain the entire routing table. • **talkDefault-listen** - RIP updates contain only a single entry. This advertises the router as the default router. • **listen-only** - No RIP updates are sent.
Cost	The cost of using this interface. RIP chooses the route with the lowest total cost (metric) for each destination.
Default Route Metric	The metric of the default route entry in RIP updates originated on this interface, if configured to **SendDefaultOnly**.

Table 20-8. RIP Interface Parameters (Continued)

Field	Description
Default Route Mode	If **talk-listen**, accepts default route entries in RIP messages received from other routes on this interface. If **talk-only**, does not accept default route entries in RIP messages received from other routes on this interface.
Split Horizon	The method for handling routes learned from this interface, when sending updates to this interface. Possible methods are: • **Poisoned Reverse** - The routes are advertised to this interface as unreachable. • **Split Horizon** - The routes are not advertised to this interface at all. • **None** - The routes are advertised to this interface as is.
Auth Type	Authentication Type. Possible methods are: • **None** • **Simple**
Auth Key	The password for this interface. This is only used if the Auth Type is set to **Simple-password**. The password may contain up to 16 characters. It may be configured here, but not viewed.

*** Note:** In the Send field, selecting '**listen-only**' or '**talk-listen**' will prevent updating the Default Route Metric field.

You can modify RIP interfaces. For more information on editing tables, refer to "Editing Tables" on page 213.

OSPF

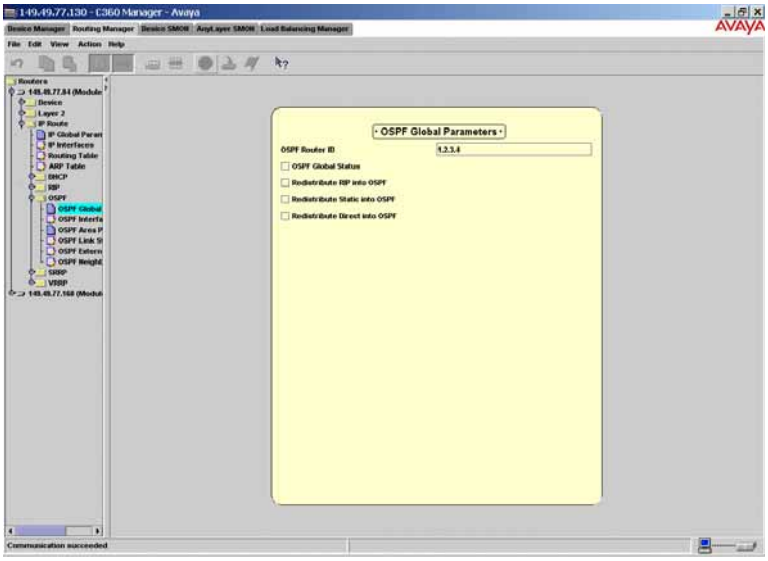
The OSPF folder provides access to the following windows:

- **OSPF Global Parameters**
- **OSPF Interfaces**
- **OSPF Area Parameters**
- **OSPF Link State Database**
- **OSPF External Database**
- **OSPF Neighbors**

OSPF Global Parameters

To define and display OSPF Global parameters, select **IP Route > OSPF > OSPF Global Parameters**. The OSPF Global Parameters window opens.

Figure 20-11. OSPF Global Parameters Window



The following parameters are displayed:

Table 20-9. OSPF Global Parameters

Field	Description
OSPF Router ID	The ID number of the router. The router ID must be unique. By default, the router ID equals one of the router's IP addresses.

Table 20-9. OSPF Global Parameters (Continued)

Field	Description
OSPF Global Status	The administrative status of OSPF in the router. If not checked, OSPF is not active on any interface, regardless of the settings in the OSPF Interfaces window.
Redistribute RIP into OSPF	Controls redistribution of routes from RIP to OSPF. If checked, all routes learned via RIP are advertised into OSPF as external routes.
Redistribute Static into OSPF	Controls redistribution of static routes into OSPF. If checked, routes are advertised into OSPF as external routes, according to the "Leak Route" definition for each static route.
Redistribute Direct into OSPF	Controls redistribution of direct routes which are external to OSPF. If checked, local subnets on which OSPF is disabled are advertised into OSPF as external routes.

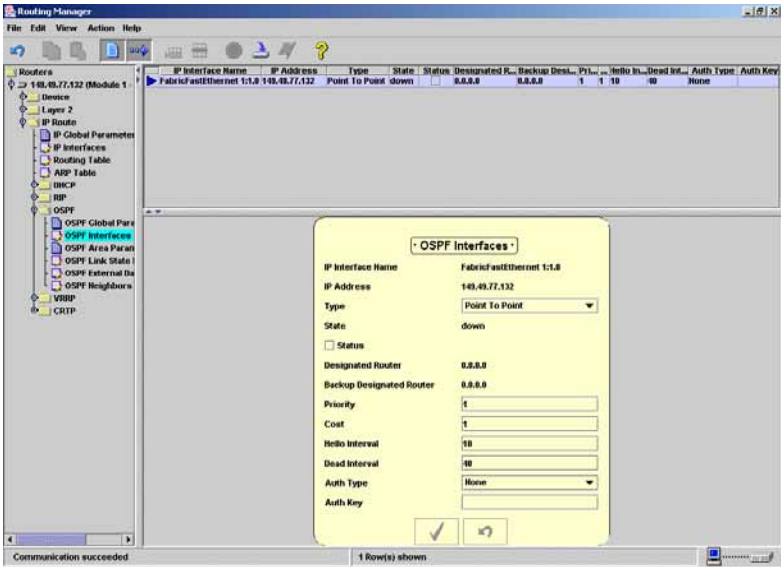
You can modify OSPF Global Parameters.

*** Note:** After updating the Router ID field, a message is displayed warning that the operation might cause the OSPF database to reset.

OSPF Interfaces

To define and display OSPF interfaces, select **IP Route > OSPF > OSPF Interfaces**. The OSPF Interfaces window opens.

Figure 20-12. OSPF Interfaces Window



The following parameters are displayed:

Table 20-10. OSPF Interfaces

Field	Description
Interface Name (not for X330WAN)	The name assigned to the selected IP interface.
IP Interface Name (X330WAN router only)	The name assigned to the selected IP interface.
IP Address	The IP address of this OSPF interface.
Type (X330WAN router only)	The type of interface: • **Point To Point** • **Point To Multipoint**

Table 20-10. OSPF Interfaces (Continued)

Field	Description
State	The interface state of the OSPF interface: • **Down** - OSPF is not active on the interface. • **Waiting** - The identity of the designated router for this subnet is not yet determined. • **Designated Router** - This router is the Designated Router on this subnet. • **Backup Designated Router** - This router is the Backup Designated Router. • **Other Designated Router** - Another router is the Designated Router on this subnet.
Status	If checked, this denotes that the interface may form neighbor relationships, and that the interface is advertised as an internal route to OSPF. If not checked, the interface is external to OSPF.
Designated Router	The IP Address of the designated router.
Backup Designated Router	The IP Address of the backup designated router.
Priority	The priority of this router to become the designated router on this interface. A value of zero indicates that this router is not eligible to become the designated router on the current network. If more than one router has the same priority, then the router ID is used.
Cost	The cost of using this interface. OSPF will choose the route with the lowest total cost (metric) to each destination.
Hello Interval	The period of time (in seconds) between Hello packets. All routers attached to a common network must have the same Hello Interval.
Dead Interval	The period of time (in seconds) that a router's Hello packets have not been seen before the router's neighbors declare the router down. All routers attached to a common network must have the same Dead interval.
Auth Type	Authentication Type. Possible methods are: • **None** • **Simple**

Table 20-10. OSPF Interfaces (Continued)

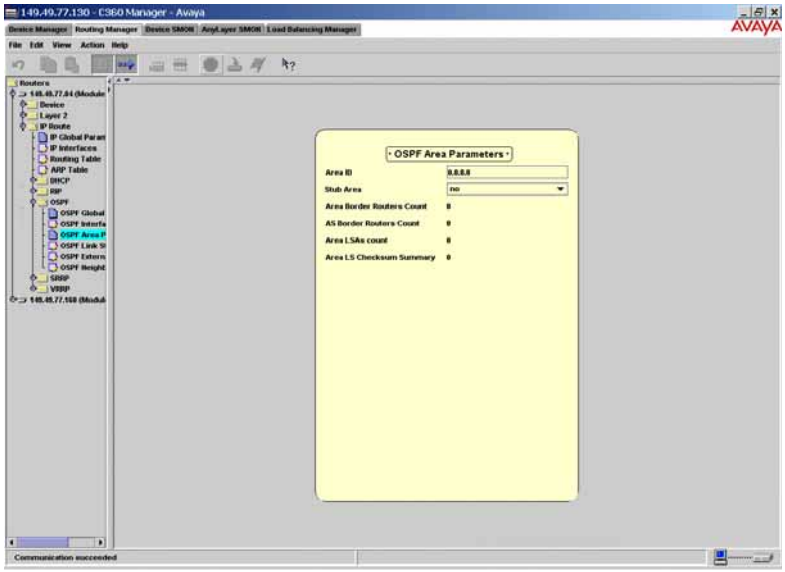
Field	Description
Auth Key	The password for this interface. This is only used if the Auth Type is set to **Simple-password**. The password may contain up to 8 characters. It may be configured here, but not viewed.

You can modify OSPF interfaces. For more information on editing tables, refer to "Editing Tables" on page 213.

OSPF Area Parameters

To define and display OSPF Area Parameters, select **IP Route > OSPF > OSPF Area Parameters**. The OSPF Area Parameters window opens.

Figure 20-13. OSPF Area Parameters Window



The following parameters are displayed:

Table 20-11. OSPF Area Parameters

Field	Description
Area ID	A unique number identifying the OSPF area to which this router belongs. Area ID 0.0.0.0 is used for the OSPF backbone.
Stub Area	If checked, external link-state advertisements are not imported into the area.

Table 20-11. OSPF Area Parameters (Continued)

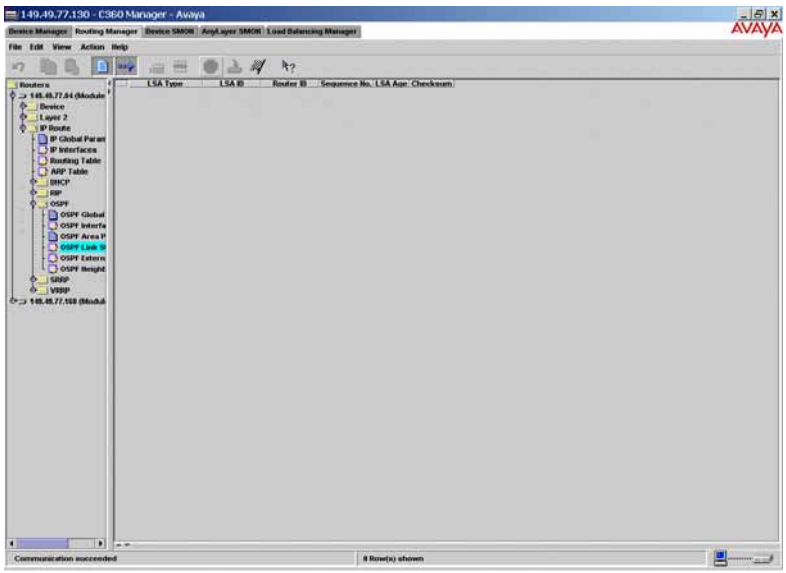
Field	Description
Area Border Routers Count	The total number of Area Border Routers reachable within this area. This number is initially zero and is calculated in each OSPF pass.
AS Border Routers Count	The total number of Autonomous System border routers reachable within this area. This number is initially zero and is calculated with each SPF pass.
Area LSAs Count	The number of link-state advertisements in the link-state database.
Area LS Checksum Summary	The sum of LS checksums of LS advertisements contained in the LS database. Use this sum to determine if there has been a change in a router's LS database, and to compare the LS database of two routers.

You can modify OSPF Area parameters.

OSPF Link State Database

To display the OSPF Link State Database, select **IP Route > OSPF > OSPF Link State Database**. The OSPF Link State Database window opens.

Figure 20-14. OSPF Link State Database Window



The following parameters are displayed:

Table 20-12. OSPF Link State Database Window

Field	Description
LSA Type	The type and format of the link state advertisement; for example, Router links and Network links.
LSA ID	Identifies the part of the routing domain that is described by the advertisement. The LSA ID can be either a router ID or an IP address.
Router ID	Identifies the originating router in the autonomous system.
Sequence No.	The sequence number of the link state advertisement. Use this parameter to detect old and duplicate link state advertisements. The larger the sequence number, the more recent the advertisement. Note that the sequence number is usually negative.
LSA Age	The age of the link state advertisement (in seconds).
Checksum	This parameter is a checksum of the complete contents of the advertisement, not including the Age value.

The parameters in the OSPF Link State Database window are read-only.

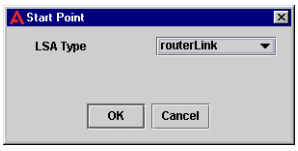
You can limit the table entries displayed. To start the display of entries from a specified interface and IP address:

1. Click .

   Or

   Select **Action > Start Point**. The Start Point dialog box opens.

Figure 20-15. OSPF Link State Database Start Point Dialog Box



2. Select an LSA Type from the LSA Type listbox.

3. Click Start. The OSPF Link State Database displays entries starting with the specified LSA Type.

To view all the entries in the OSPF Link State Database:

Click .

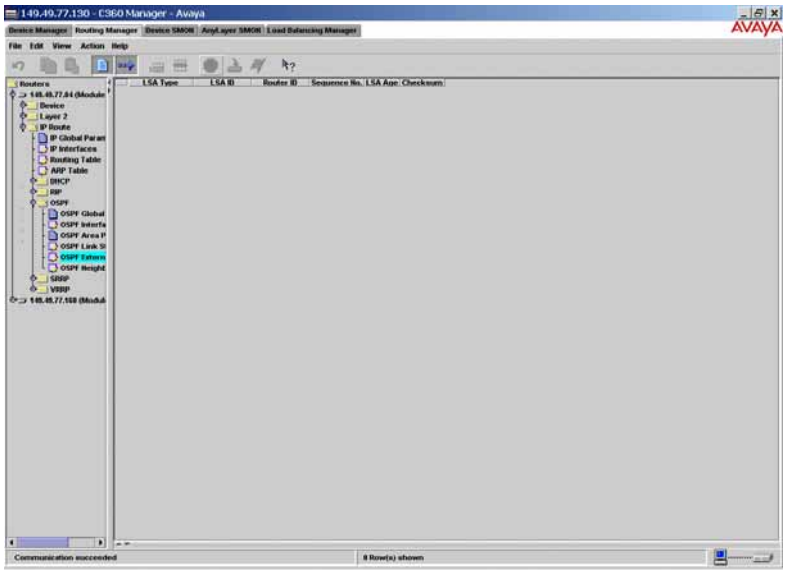
Or

Select **View > Refresh**. All entries appear in the table.

OSPF External Database

To display the OSPF External Database window, select **IP Route > OSPF > OSPF External Database**. The OSPF External Database window opens.

Figure 20-16. OSPF External Database Window



The following parameters are displayed:

Table 20-13. OSPF External Database Window

Field	Description
LSA Type	The type and format of the link state advertisement; for example, Router links and Network links.
LSA ID	Identifies the part of the routing domain that is described by the advertisement. The LSA ID can be either a router ID or an IP address.

Table 20-13. OSPF External Database Window (Continued)

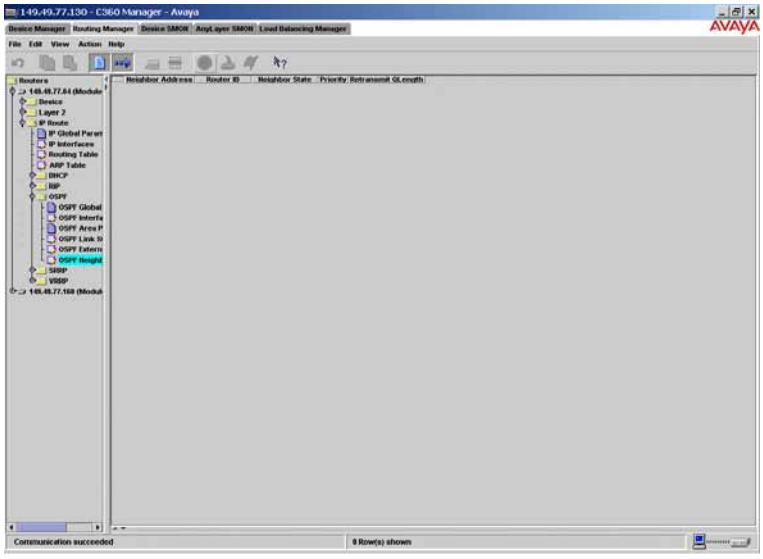
Field	Description
Router ID	Identifies the originating router in the autonomous system.
Sequence No.	The sequence number of the link state advertisement. Use this parameter to detect old and duplicate link state advertisements. The larger the sequence number, the more recent the advertisement. Note that the sequence number is usually negative.
LSA Age	The age of the link state advertisement (in seconds).
Checksum	This parameter is a checksum of the complete contents of the advertisement, not including the Age value.

The parameters in the OSPF External Database window are read-only.

OSPF Neighbors

To display the OSPF Neighbors window, select **IP Route > OSPF > OSPF Neighbors**. The OSPF Neighbors window opens.

Figure 20-17. OSPF Neighbors Window



The following parameters are displayed:

Table 20-14. OSPF Neighbors Parameters

Field	Description
Neighbor Address	The IP address of this neighbor.
Router ID	The unique OSPF identifier for the neighboring router.
Neighbor State	The state of the relationship with this neighbor: • **Down** • **Attempt** • **Init** • **Two Way** • **Exchange Start** • **Exchange** • **Loading** • **Full**
Priority	The priority of this neighbor in the Designated Router election.
Retransmit QLength	The current length of the retransmission queue.

The parameters in the OSPF Neighbors Table window are read-only.

VRRP

The VRRP folder provides access to the following windows:

- **VRRP Global Parameters**
- **VRRP Table**

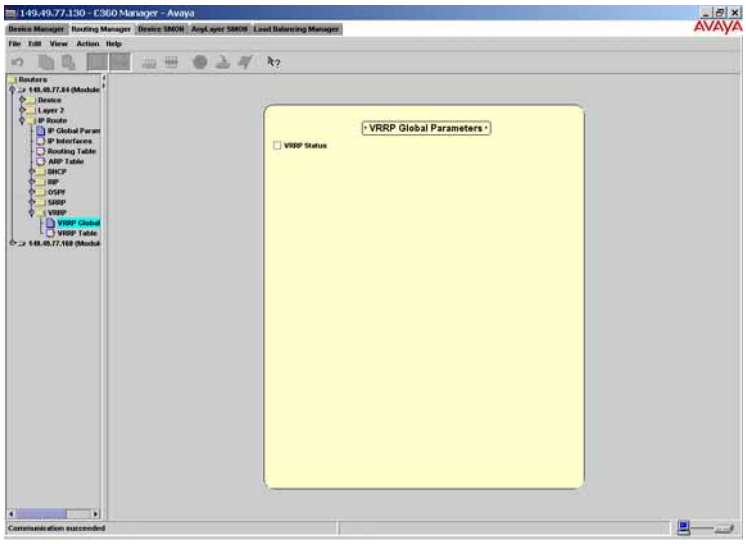
VRRP Global Parameters

VRRP (Virtual Router Redundancy Protocol) provides a method for configuring a redundancy between routers. A Master Router is selected for each Virtual Router. Backup routers function normally, while checking the Master Router. If the Master Router fails, the backup routers handle traffic directed to the Master Router.

*** Note:** VRRP and SRRP are mutually exclusive.

To define and display the VRRP global parameters, select **IP Route > VRRP > VRRP Global Parameters**. The VRRP Global Parameters window opens.

Figure 20-18. VRRP Global Parameters Window



The following parameter is displayed:

Table 20-15. VRRP Global Parameter

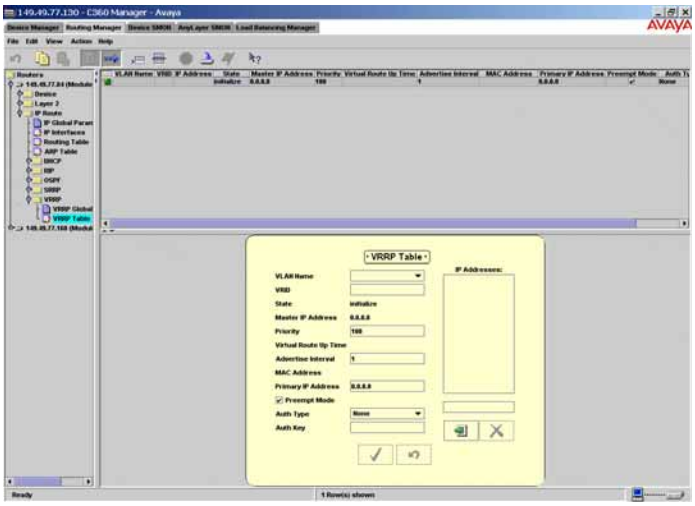
Field	Description
VRRP Status	When the VRRP global parameter checkbox is checked, VRRP is operational on the router. If unchecked, VRRP is not operational on the router.

You can modify the VRRP Global Parameter.

VRRP Table

To define and display the VRRP table, select **IP Route > VRRP > VRRP Table**. The VRRP table opens.

Figure 20-19. VRRP Table



The following parameters are displayed:

Table 20-16. VRRP Table Parameters

Field	Description
VLAN Name (not for X330WAN)	The name of the selected interface.
L2 Interface Name (X330WAN router only)	The name of the selected interface.
VRID	A number which, along with an interface index (ifIndex), serves to uniquely identify a virtual router on a given VRRP router. A set of one or more associated addresses is assigned to a VRID.
IP Address	The IP address associated with this virtual router. If more than one IP address is associated with this virtual router, **`Click for Details`** appears in the IP Address field. Clicking the field opens the Form View showing all IP addresses associated with this virtual router. The IP addresses must be on a local subnet on the VLAN.

Table 20-16. VRRP Table Parameters (Continued)

Field	Description
State	The state of the virtual router. Possible states are: • **initialize** - The virtual router is not functional. • **backup** - The virtual router is monitoring the availability of the master router. • **master** - The virtual router is forwarding packets with IP addresses associated with this virtual router.
Master IP Address	The IP address of the physical router currently acting as the Virtual Router's Master Router.
Priority	This object specifies the priority to be used for the virtual router master election process. Higher values imply higher priority. A priority of '0', although not settable, is sent by the master router to indicate that this router has ceased to participate in VRRP and a backup virtual router should transition to become a new master. A priority of 255 is used for the router that owns the associated IP address(es).
Virtual Route Up Time	The time when the virtual router's state changed from initialized to backup or master. The time is expressed in ticks (1/60 of a second).
Advertise Interval	The interval, in seconds, between VRRP advertisement messages sent by the master router.
MAC Address	The virtual MAC address of the virtual router.
Primary IP Address	The physical router's IP address to be used if it is elected to be Master Router. The Primary IP Address must belong to the physical router and be on the selected VLAN. If this parameter is set to 0.0.0.0, the IP address which is numerically lowest will be selected.
Preempt Mode	If checked, the virtual router with the highest priority will preempt active routers and become the master router.

Table 20-16. VRRP Table Parameters (Continued)

Field	Description
Auth Type	Authentication Type. Possible methods are: • **None** • **Simple**
Auth Key	The password for this interface. This is only used if the Auth Type is set to **Simple**. The password may contain up to 8 characters. It may be configured here, but not viewed.

To associate IP addresses with a selected virtual router:

1. Select a virtual router in the VRRP table.
2. Ensure that the Form View is visible.
3. Enter the IP address to associate with the selected router in the textbox under the IP Addresses listbox in the Form View.
4. Click . The IP address is associated with the virtual router.

To disassociate IP addresses from a selected virtual router:

1. Select a virtual router in the VRRP table.
2. Ensure that the Form View is visible.
3. Select the IP address from the IP Addresses listbox in the Form View.
4. Click . The IP address is no longer associated with the virtual router.

You can modify VRRP parameters. For more information on editing tables, refer to "Editing Tables" on page 213.

CRTP

The CRTP folder provides access to the following window:

- **CRTP Interfaces**

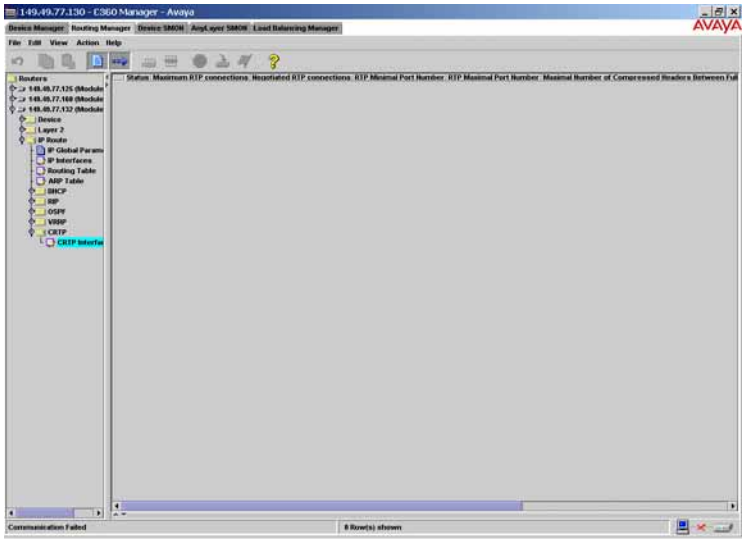
CRTP Interfaces

The Avaya X330WAN router supports RTP compression, reducing the overhead of transmitting voice packets over the E1/T1 line. You can configure CRTP (Compressed RTP) parameters for each PPP interface on the X330WAN router.

*** Note:** The CRTP Interfaces window is only available on an X330WAN router.

To define and display CRTP Interfaces, select **IP Route > CRTP > CRTP Interfaces**. The CRTP interfaces window appears.

Figure 20-20. CRTP Interfaces WIndow



The following parameters are displayed:

Table 20-17. CRTP Interface Table Parameters

Field	Description
Layer 2 Interface Name	The name of the selected interface.

Table 20-17. CRTP Interface Table Parameters (Continued)

Field	Description
Status	The status of RTP compression on this interface. Possible statuses include: • **Enabled** - RTP compression is enabled on the interface. • **Disabled** - RTP compression is disabled on the interface.
Maximum RTP Connection	The maximum number of context identifiers for RTP connections on this interface. 0 means that no RTP headers will be compressed.
Actual RTP Connections	The actual number of context identifiers for RTP connections on this interface.
Min Port	The minimal UDP destination port number to be considered as RTP traffic.
Max Port	The maximal UDP destination port number to be considered as RTP traffic.
Max Interval	The maximum number of seconds between full headers.
Max Time	The maximum number of compressed packets that can be sent between full headers.
Compression Ratio	The average ratio between the compressed header size and the original header size on this interface. The value is expressed as a percentage.
Maximum TCP Connection	The maximum number of context identifiers for TCP connections on this interface.
Actual TCP Connections	The actual number of context identifiers for TCP connections on this interface.

You can modify CRTP parameters on PPP interfaces. For more information on editing tables, refer to "Editing Tables" on page 213.

A Menus

This appendix gives the full structure of the menus in the Avaya C360 Manager.

Device Manager Menus

This section provides the menu structure of the Avaya C360 Device Manager.

File Menu

Table A-1. File Menu - Device Manager

Item	Description
Exit	Exits the Avaya C360 Manager.

View Menu

Table A-2. View Menu - Device Manager

Item	Description
Refresh	Refreshes the display with information from the device.
Configuration	Switches the Device Manager to configuration mode.
Port RMON	Switches the Device Manager to monitoring mode.
Switch Connected Addresses	Displays a list of stations connected to each of the device's ports.
Toolbars > Show Application Toolbar	Toggles the display of the application toolbar.
Toolbars > Show Get/Set Toolbar	Toggles the display of the Get/Set toolbar.

Configure Menu

Table A-3. Configure Menu - Device Manager

Item	Description
Stack Configuration	Displays information for the device.
VLANs	Displays and enables configuration of VLANs.
LAG	Displays and enables configuration of LAGs.
Port Redundancy	Displays and enables configuration of port redundancies.
Port Mirroring	Allows copying of all transmitted and received packets from one port to another.
Trap Managers	Displays managers and traps configuration information.
IP Multicast Filtering	Displays the IP Multicast Filtering dialog box.
MAC Port Security	Displays and enables configuration of MAC Port Security.
WAN > Channel Groups	Opens the Channel Groups table.
WAN > Commit	Saves the updated configuration to the X330WAN expansion module.
WAN > Backup Interfaces	Opens the Backup Interfaces table.
Media Gateway > VoIP Configuration	Opens the VoIP config tab of the VoIP Engine Dialog box.

Actions Menu

Table A-4. Actions Menu - Device Manager

Item	Description
802.1x > Initialize Selected Ports	Initializes 802.1x security on the selected ports.
802.1x > Initialize All Ports	Initializes 802.1x security on all ports.
802.1x > Reauthenticate Selected Ports	Forces reauthentication of 802.1x security on the selected ports.
802.1x > Reauthenticate All Ports	Forces reauthentication of 802.1x security on all ports.
Reset Device	Resets the entire device.

Table A-4. Actions Menu - Device Manager (Continued)

Item	Description
Reset Module(s)	Resets the selected modules.
Reset Media Module(s)	Reset the selected media modules.
Reset WAN Plugin(s)	Reset the selected X330WAN expansion modules.
Clear CAM	Clear the Avaya C360 devices's CAM table of all learned MAC addresses.

Tools Menu

Table A-5. Tools Menu - Device Manager

Item	Description
Administer Station/Gateway	Opens Avaya Site Administrator on the station or the selected Media Gateway.
Administer Call Controller	Opens Avaya Site Administrator on the selected Media Call Controller.

Help Menu

Table A-6. Help Menu - Device Manager

Item	Description
Help Contents	Opens the on-line help contents page.
Help On	Activates context sensitive help.
About Avaya C360 Device Manager	Copyright information about the Avaya C360 Device Manager.

Routing Manager Menus

This section provides the menu structure of the Avaya C360 Routing Manager.

File Menu

Table A-7. File Menu - Routing Manager

Item	Description
Save	Saves the current table to a text file.
Commit	Saves the current configuration to the router.

Edit Menu

Table A-8. Edit Menu - Routing Manager

Item	Description
Undo	Undoes changes made to the table or form currently displayed.
Copy	Copies the selected information to the clipboard.
Paste	Pastes information from the clipboard into the selected table row.
Insert Row	Adds a row to the table.
Delete Row	Deletes the selected table row.

View Menu

Table A-9. View Menu - Routing Manager

Item	Description
Refresh	Refreshes the information in the current table.
Form	Toggles the display of a form corresponding to the current table.
More	Toggles the display of additional table parameters.

Action Menu

Table A-10. Action Menu - Routing Manager

Item	Description
Stop	Stops loading information into the current table.
Apply	Sends the configuration information to the device.
Start Point	Opens the Start Point dialog box for specifying the starting point of entries displayed in the table.
Reset	Reset the selected router.

Help Menu

Table A-11. Help Menu - Routing Manager

Item	Description
Context Sensitive Help	Activates context sensitive help.
Contents	Opens the on-line help contents page.
About Routing Manager	Copyright information about the Avaya C360 Routing Manager.

B Web Management

This appendix provides instructions for managing Avaya C360 Devices via the Internet and contains the following topics:

- **Web Management Overview** - An overview on Web Management.
- **Configuring the Avaya C360 Device** - Instructions on how to configure the Avaya C360 Device for the first time.

Web Management Overview

Web Management provides a simple method of managing Avaya C360 Devices via the Internet. The Avaya C360 Manager software does not need to be installed on your computer.

Instead, a small plug-in for your web browser activates the embedded manager software. This plug-in loads automatically when you use Web Management.

*** Note:** Port RMON is not available via Web Management.

On-line help is only available if you have installed the on-line help on your network and configured the Avaya C360 Device with the location of the help files. For information on installing the on-line help and configuring the device with the location of the files, refer to the *Avaya C360 User's Guide*.

Configuring the Avaya C360 Device

When an Avaya P330ML or C360 module is initially configured as a full router, it must be assigned an IP address. The IP address must be assigned using the CLI (Command Line Interface) setup screens. For information on assigning an IP address to the router module, refer to the *Avaya C360 User's Guide*.

Index

Numerics
802.1x port security 199

A
Adding
  a Port Redundancy 162
  managers to table 193
  table entries 213
Additional table parameters
  viewing 212
Advanced tab
  Channel Group 87
  USP 108
Application tabs 4
Application Toolbar buttons 210
Applying changes
  in tables 5
  IP Multicast Filtering configuration 181
  Port Redundancy 169
  VLAN configuration 147
ARP Table window 229
Avaya C360 Management
  connected stations 195
  device configuration 19
  G700 Media Gateway 59
  introduction 1
  IP Multicast Filtering 179
  LAGs 149
  PoE 53
  Port Mirroring 171
  Port Redundancy 159
  port RMON 131
  trap managers 183
  VLANs 135
  VoIP Engine configuration 71
  WAN configuration 79
  welcome to Avaya C360 Manager xi
Avaya C360 Manager
  Application tabs 4
  Device Manager 7
  modes 15
  overview 1
  starting 2
  Status Line 5
  user interface 4
Avaya Site Administration (ASA) 68

B
Backup interface
  configuration 122
  create 123
  delete 123
  table 122
Backup Interface Parameters screen 127
Backup Interface Wizard 124
  Backup Interface Parameters screen 127
  Confirmation screen 128
  Select Backup Interface screen 127
  Select Module screen 125
  Select Primary Interface screen 126
  Welcome screen 125
Base Port Selection screen 153

C
Channel Group
  Advanced tab 87
  Channel Group tab 85
  creating 101
  deleting 101
  dialog box 99
  DLCIs tab 96
  editing 101
  frame relay information 90
  Frame Relay tab 91
  managing 99
  PPP session information 84
  PPP tab 88
  Sub-Frame-Relays tab 93
  viewing information 84
  viewing table 99
Channel Group Wizard 101
  Confirmation screen 105
  Select Channels and Speed screen 104
  Select E1/T1 Port screen 103

Select Name and Encapsulation screen 102
Welcome screen 102
Chassis View 12
Application Toolbar 8
colors in 12
Get/Set Toolbar 10
selecting elements 14
Status Line 5
Committed changes 214
Configurable router 208
Configuration
applying changes 214
committed changes 214
PVID 147
running changes 214
saving changes 214
Configuring
a port's VLAN configuration 140
backup interfaces 122
devices 19
devices via the Internet 261
frame relay Channel Groups 90
G700 60
G700 Media Gateway modules 60
IP Multicast Filtering 180
LAGs 31
media module 67
modules 24
PoE information 54
PoE modules 55
PoE ports 56
Port Mirroring 171
ports 39
PPP session Channel Groups 84
trap managers 183
USP 105
USP frame relay interface 114
USP PPP interface 106
VLAN settings for ports 146
VLANs 142
VoIP 76
VoIP Engine 71
WAN 79
WAN E1/T1 port 81
X330WAN module 80
Confirmation screen
Backup Interface Wizard 128
Channel Group Wizard 105
LAG Wizard 156
Port Mirroring Wizard 178
Port Redundancy Wizard 168
Contents page in Help 17, 215
Contracting
VLAN tree branch 138
Create Welcome screen 173
Creating
backup interface 123
Channel Groups 101
DLCIs 120
LAGs 151
Sub-Frame-Relays 117
table entries 213
VLANs 142
CRTP
CRTP Interfaces window 253
overview 253
CRTP Interfaces window 253

D

Deleting
backup interface 123
Channel Groups 101
DLCIs 121
LAGs 157
managers from table 193
Port Redundancies 169
Sub-Frame-Relays 118
table entries 213
VLANs 145
Desktop 11
Destination Port Selection screen 176
Device
configuration 19
Global Parameters window 217
information 20
overview 217
refreshing information 16
resetting 51
Device Manager
Application Toolbar 8
Chassis View 12
Desktop 11
Dialog Area 15
Get/Set Toolbar 10
help 17
menus 255
overview 7
Toolbar 8

Tree View 11
user interface 7
DHCP
DHCP/BOOTP Global Parameters window 231
DHCP/BOOTP Parameters window 232
overview 231
Dialog Area 15
Dialog box symbols 16
Discarding
Port Redundancy changes 169
Distributing high-bandwidth applications 179
DLCI
creating 97, 120
deleting 98, 121
modifying 97, 120
DLCIs tab
Channel Group 96
USP 120
Dragging and dropping for PVID configuration 147

E

E1/T1 port configuration 81
Edit/Delete Welcome screen 174
Editing
Channel Groups 101
LAGs 151
table entries 213
tables 213
the Trap Managers table 193
trap status 193
VLAN names 143
Expanding
VLAN tree branch 138

F

Folder
CRTP 253
Device 217
DHCP 231
IP Route 221
Layer 2 219
OSPF 239
RIP 234
VRRP 248
Form Area
resizing 212
Routing Manager 212
Frame relay
viewing information 90
Frame Relay tab
Channel Group 91
USP 114
Frames Direction Selection screen 177

G

G700 Media Gateway
Avaya Site Administration 68
device configuration 60
media module configuration 67
MG Config tab 61
MGC Config tab 65
MGP Config tab 62
module configuration 60
overview 59
Switch Config tab 60
GBIC ports 13
Get/Set Toolbar 10
Graph
Port RMON traffic 132
scrolling within 133
unfreezing 133
zooming in and out 133
Guide
intended users xi
organization xi
purpose xi

H

Help
contents page 17, 215
Routing Manager 215
topic 17, 215
using 17
Hiding additional table parameters 212
How this guide is organized xi
How to
access the VLAN Configuration dialog box 137
configure backup interfaces 122
configure devices 19
configure WAN 79
scroll within the graph 133
select elements 14
sort the list of switch connected addresses 197

unfreeze the graph 133
use on-line help 215
use the Device Manager Application Toolbar 8
use the Get/Set Toolbar 10
view backup interfaces 122
zoom in and out of the graph 133

I
Internet management
configuration 261
overview 261
Introduction
Avaya C360 Manager xi
IP Global Parameters window 222
IP Interfaces window 223
IP Multicast Filtering
applying configuration changes 181
changing parameters 181
configuring 180
overview 179
refreshing the dialog box 181
IP Route
ARP Table 229
CRTP 253
CRTP Interfaces window 253
DHCP 231
DHCP/BOOTP Global Parameters window 231
DHCP/BOOTP Parameters window 232
IP Global Parameters 222
IP Interfaces 223
OSPF 239
OSPF Area Parameters window 243
OSPF External Database window 246
OSPF Global Parameters window 239
OSPF Interfaces window 241
OSPF Link State Database window 244
OSPF Neighbors window 247
overview 221
RIP 234
RIP Global Parameters window 234
RIP Interfaces window 236
Routing Table 225
VRRP 248
VRRP Global Parameters window 249
VRRP Table window 250

L
L2 Interfaces window 219
LAG Name screen 155
LAG Wizard 151
Base-Base Port Selection screen 153
Confirmation screen 156
LAG Name screen 155
Member Port Selection screen 154
Welcome screen 152
LAGs
colors 12
configuration 31
creating 151
deleting 157
editing 151
overview 149
selecting 14
viewing the LAG table 150
Layer 2
L2 Interfaces window 219
overview 219
VLANs window 219
Link Aggregation Groups, *see* LAGs

M
Manager
Routing 207
trap 183
Managing
Channel Groups 99
devices via the Internet 261
tables 5
Manual
intended users xi
organization xi
purpose xi
Master VLAN list 136
Media Gateway
G700 59
Media Gateway Controller
IP settings 65
MGC List 65
Media Gateway Processor
general information 62
IP address settings 63
QoS parameters 64
VLAN settings 63
Media module configuration 67
Member Port Selection screen 154

Menus
  Device Manager 255
  Routing Manager 258
  structure 255
MG Config tab 61
MGC Config tab 65
MGC List 65
MGP Config tab 62
Modes
  Configuration 15
  Port RMON 15
  Router 208
  routing 208
  Second Layer 208
  switching between 15
Modifying
  DLCIs 120
  Sub-Frame-Relays 118
  table entries 213
Module
  colors 12
  configuration 24
  configuring PoE 55
  resetting 51
  selecting 14
  X330WAN configuration 80
Monitoring
  performance 131
  traffic 132
  traffic through a specific port 171
More table parameters
  viewing 212

N
Name and Type screen 167

O
OpenView (Solaris) 2
Organization of guide xi
OSPF
  Area Parameters window 243
  External Database window 246
  Global Parameters window 239
  Interfaces window 241
  Link State Database window 244
  Neighbors window 247
  overview 239
Overview
  LAGs 149
  PoE 53
  Port Mirroring 171
  Port Redundancy 159
  switch connected addresses 195
  trap managers 183
  VLAN configuration 135
  VLANs 136
  VoIP 71
  X330WAN module 79

P
Pie chart 132
PoE
  configuring modules 55
  configuring ports 56
  overview 53
  viewing configuration 54
  viewing information 54
Port
  colors 12
  configuration 39, 146
  Configuration Area 140
  configuring PoE 56
  E1/T1 configuration 81
  GBIC 13
  PVID configuration 147
  redundancy *see* Port Redundancy
  selecting 14
  selecting for VLAN configuration 145
  viewing PoE information 54
  viewing VLAN configuration 146
  VLAN settings 145
Port Mirroring
  configuring 171
  overview 171
Port Mirroring Wizard
  Confirmation screen 178
  Create Welcome screen 173
  Destination Port Selection screen 176
  Edit /Delete Welcome screen 174
  Frames Direction Selection screen 177
  overview 172
  Source Port Selection screen 175
Port Redundancy
  adding 162
  deleting 169
  overview 159
  updating table 169

viewing the Port Redundancy dialog box 160
Port Redundancy Wizard
Confirmation screen 168
Name and Type screen 167
overview 163
Primary Port Selection screen 165
Secondary Port Selection screen 166
Welcome screen 164
Port RMON
overview 131
pie chart 132
traffic graph 132
window 132
Power over Ethernet
see PoE
PPP session
viewing information 84
PPP tab
Channel Group 88
USP 112
Primary Port Selection screen 165

R

Refreshing
device information 16
IP Multicast Filtering dialog box 181
Port Redundancy dialog box 169
tables 5
Removing
managers from table 193
table entries 213
Renaming VLANs 143
Resetting
devices 51
modules 51
routers 215
Resizing
Form Area 212
Table Area 212
RIP
Global Parameters window 234
Interfaces window 236
overview 234
Router mode 208
Routing Manager
Form Area 212
help 215
introduction 207
menus 258
resetting 215
Router mode 208
routing modes 208
Second Layer mode 208
Table Area 212
Toolbar 210
Tree View 211
user interface 209
Routing modes
overview 208
Router 208
Second Layer 208
Routing Table window 225
Running Avaya C360 Manager
from Avaya MultiService Console 2
from HP NNM 2
via the Internet 3
Running changes 214

S

Saving
table information as text 214
Scrolling within the graph 133
Second Layer mode 208
Secondary Port Selection screen 166
Security
802.1x port 199
Select Backup Interface screen 127
Select Channels and Speed screen 104
Select E1/T1 Port screen 103
Select Module screen 125
Select Name and Encapsulation screen 102
Select Primary Interface screen 126
Selecting
elements 14
ports for VLAN configuration 145
traffic to monitor 133
Selection List 139
Serial Port tab 106
Shortcuts
Routing Manager Toolbar 210
Sorting the list of stations 197
Source Port Selection screen 175
Starting
Avaya C360 Manager 2
Avaya C360 Manager using MSNM 2
Web management 3
Station connections 195

Status
GBIC ports 13
Line 5
tab, VoIP 77
Sub-Frame-Relay
creating 94, 117
deleting 94, 118
modifying 94, 118
Sub-Frame-Relays tab
Channel Group 93
USP 117
Switch Config tab 60
Switch connected addresses
overview 195
sorting list 197
window 196
Switching views 4
Symbols in tables 5
Synchronizing VLAN names 144

T
Table
adding and deleting managers 193
apply changes 5, 213
Backup Interfaces 122
Channel Group 99
Device Trap Managers 184
editing manager status 193
editing Trap Managers 193
LAGs 150
Media Gateway Trap Managers 189
Port Redundancy 160
refreshing 5
row symbols 5
saving as text 214
Selection List 139
undoing changes 5, 213
using 16
WAN Trap Managers 191
Table Area
in Routing Manager 212
resizing 212
Table Entries
Adding 213
Creating 213
Deleting 213
Editing 213
Modifying 213
Removing 213
Tagging packets with VLAN information 136
Text files
saving table information to 214
Toolbar
Device Manager Application 8
Device Manager Get/Set 10
Routing Manager 210
Traffic
Port RMON graph 132
types 133
viewing statistics 133
Trap managers
configuration 183
overview 183
Trap Managers table
adding and deleting managers 193
device 184
editing 193
editing status 193
Media Gateway 189
WAN 191
Traps
device 184
editing status 193
Media Gateway 189
WAN 191
Tree View
Device Manager 11
Routing Manager 211
Types of traffic 133

U
Undo changes in table 213
Unfreezing the graph 133
Updating
changes in table 213
Port Redundancy dialog box 169
User interface
Avaya C360 Manager 4
Device Manager 7
Routing Manager 209
Users of Avaya C360 management xi
Using
Avaya C360 help 17
Chassis View 12
Device Manager Application Toolbar 8
dialog boxes 16
Get/Set Toolbar 10
on-line help 215

tables 16
USP
Advanced tab 108
configuration 105
DLCIs tab 120
frame relay interface 114
Frame Relay tab 114
PPP interface 106
PPP tab 112
Serial Port tab 106
Sub-Frame-Relays tab 117
viewing information 105

V
Viewing
additional table parameters 212
backup interfaces 122
Channel Group information 84
Channel Group table 99
connected stations 195, 196
device information 20
device traps 184
E1/T1 port configuration 81
expansion module configuration 80
frame relay Channel Group information 90
LAG configuration 31
LAG table 150
Media Gateway traps 189
module configuration 24
port configuration 39
port VLAN configuration 146
PPP session Channel Group information 84
Switch Connected Addresses window 196
the Port Redundancy dialog box 160
the Port RMON window 132
traffic statistics 133
USP information 105
VLAN list 137
WAN traps 191
VLANs
accessing the dialog box 137
applying configuration changes 147
configuration 135
creating 142
creating, deleting, and renaming 142
deleting 145
expanding and contracting tree 138
managing 142
master VLAN list 136
overview 136
Port Configuration Area 140, 146
port PVID configuration 147
port VLAN settings 145
renaming 143
selecting ports for VLAN configuration 145
Selection List 139
synchronizing names 144
tags 136
tree 138
viewing configuration 137
viewing port VLAN configuration 146
VLAN tree 138
window 219
VoIP
configuration 76
configuring the engine 71
general engine information 72
overview 71
QoS 73
Resources tab 72
RSVP 75
RTCP 74
status tab 77
VRRP
Global Parameters window 249
overview 248
Table window 250

W
WAN
configuration 79
X330WAN overview 79
Web management
configuration 261
overview 261
starting 3
Welcome screen
Backup Interface Wizard 125
Channel Group Wizard 102
LAG Wizard 152
Port Redundancy Wizard 164
Welcome to Avaya C360 Manager xi
Who should use Avaya C360 Manager xi
Window
ARP Table 229
CRTP Interfaces 253

Device Global Parameters 217
DHCP/BOOTP Global Parameters 231
DHCP/BOOTP Parameters 232
IP Global Parameters 222
IP Interfaces 223
IP Routing Table 225
L2 Interfaces 219
OSPF Area Parameters 243
OSPF External Database 246
OSPF Global Parameters 239
OSPF Interfaces 241
OSPF Link State Database 244
OSPF Neighbors 247
Port RMON 132
RIP Global Parameters 234
RIP Interfaces 236
Switch Connected Addresses 196
VLANs 219
VRRP Global Parameters 249
VRRP Table 250
Wizard
Backup Interface 124
Channel Group 101
LAG 151
Port Mirroring 172
Port Redundancy 163

X

X330WAN
module configuration 80
overview 79

Z

Zooming in and out of the graph 133